COORDINADORES
Joan Balcells Padullés
Agustí Cerrillo i Martínez
Miquel Peguera Poch
Ismael Peña López
María José Pifarré de Moner
Mònica Vilasau Solana

Internet, Derecho y Política
Una década de transformaciones

Actas del X Congreso Internacional Internet, Derecho y Política.
Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014

Internet, Law & Politics
A Decade of Transformations

Proceedings of the 10th International Conference on Internet, Law & Politics.
Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014

UOC
Universitat Oberta de Catalunya
HUYGENS EDITORIAL

Internet, Derecho y Política. Una década de transformaciones

Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014

Internet, Law & Politics. A Decade of Transformations

Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014

2014

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS EDITORIAL

INTERNET, DERECHO Y POLÍTICA.
UNA DÉCADA DE TRANSFORMACIONES

INTERNET, LAW & POLITICS.
A DECADE OF TRANSFORMATIONS

COORDINADORES

Joan Balcells Padullés, Agustí Cerrillo-i-Martínez, Miquel Peguera Poch
Ismael Peña-López, María José Pifarré de Moner y Mònica Vilasau Solana

© 2014, Huygens Editorial
La Costa, 44-46, át. 1ª
08023 Barcelona
www.huygens.es

ISBN: 978-84-697-0826-2
Editado en España

Índice General

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y DEFENSA DE LOS CONSUMIDORES

COMUNICACIONES SOBRE CIBERCRIMINALIDAD

COMUNICACIONES SOBRE ADMINISTRACIÓN ELECTRÓNICA

Presentación

Joan Balcells Padullés
Agustí Cerrillo i Martínez
Miquel Peguera Poch
Ismael Peña López
María José Pifarré de Moner
Mònica Vilasau Solana
Profesores de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya

El Congreso Internet, Derecho y Política llega este año a su décima edición. En estos diez años ha constituido un foro académico internacional de reflexión sobre la impacto de las tecnologías de la información y la comunicación en el ámbito del derecho y de la ciencia política, en particular en campos como la propiedad intelectual, la libertad de expresión, la privacidad, la administración pública, el comercio electrónico, la criminalidad o la participación política. En este tiempo hemos sido observadores privilegiados de las transformaciones en el derecho y la política derivadas de los nuevos fenómenos que iban surgiendo, como la web 2.0, las redes sociales, el *cloud computing* o el *Big Data*.

Han sido diez años en los que el desarrollo de la tecnología y su uso por la sociedad han generado tensiones en la regulación vigente, pensada para un escenario pre-digital. Pero también han sido diez años de reivindicación del derecho como mecanismo para dar solución a los nuevos conflictos que surgen en Internet, buscando un equilibrio satisfactorio entre los distintos intereses implicados. Desde la perspectiva de la ciencia política, estos diez años han permitido observar la aparición de nuevos canales para la participación política y de mayores posibilidades para la transparencia y la rendición de cuentas por parte de los poderes públicos. Además, a lo largo de este periodo, las TIC también han sido el motor de movilizaciones sociales, como el 15-M o la primavera árabe, que han transformado el panorama político nacional e internacional.

En el presente libro de actas se recogen las comunicaciones que, tras un proceso de revisión por pares, han sido aceptadas para el Congreso. Se distribuyen en seis bloques temáticos (propiedad intelectual, privacidad y protección de datos, comercio electrónico y defensa de los consumidores, cibercriminalidad, administración electrónica, y política e Internet).

Deseamos mostrar nuevamente nuestro agradecimiento a todos los investigadores que han contribuido con sus aportaciones, así como renovar nuestro compromiso de seguir en primera línea del debate académico internacional en este apasionante campo de investigación.

COMUNICACIONES SOBRE PROPIEDAD INTELECTUAL

1

DERECHOS FUNDAMENTALES Y OBSERVANCIA DE PROPIEDAD INTELECTUAL

Xavier Seuba Hernández
Investigador Senior en (IN3),
Universitat Oberta de Cataluña

RESUMEN: Las relaciones entre derechos humanos y derechos de propiedad intelectual han sido objeto de especial atención en el último quindenio, atención que se ha centrado en el ámbito sustantivo de tales relaciones y ha descuidado las normas sobre observancia de la propiedad intelectual. La proliferación de detalladas y exigentes obligaciones en materia de observancia hace necesaria, cuando no urgente, la sistematización de tales relaciones. En este artículo se analizan el derecho a un recurso, las medidas de protección de prueba y las sanciones penales en caso de infracción de derechos de propiedad intelectual para describir las que pueden ser relaciones positivas, ambiguas o negativas entre derechos humanos y observancia de la propiedad intelectual. Asimismo, se propone recurrir a las normas secundarias de derecho internacional público para abordar las interacciones descritas.

PALABRAS CLAVE: Observancia; propiedad intelectual; derechos humanos; medidas de preservación de prueba; sanciones penales; conflicto.

1. OBSERVANCIA DE LA PROPIEDAD INTELECTUAL Y DERECHOS HUMANOS

1.1. El descuido y creciente atención a la relación entre derechos humanos y observancia de la propiedad intelectual

Las relaciones entre derechos humanos y derechos de propiedad intelectual han sido objeto de especial atención en los últimos quince años. En el plano internacional, la proliferación de tratados con disposiciones detalladas y exigentes en materia de propiedad intelectual ha causado preocupación en numerosos foros de derechos humanos, en particular debido al impacto de tales tratados sobre el acceso a bienes públicos y sobre la protección de garantías fundamentales relacionadas con las libertades civiles. Esta atención se ha visto acentuada por la celebración de acuerdos comerciales preferenciales (ACPs) con cada vez más y más estrictas disposiciones en materia de propiedad intelectual.

Hasta la fecha la mayoría de los análisis sobre la interacción entre propiedad intelectual y derechos humanos se han centrado en cuestiones relacionadas con el contenido sustantivo de la propiedad intelectual, fundamentalmente las implicaciones del derecho de exclusión concedido a los titulares. De ahí que la atención se haya centrado en la

interacción entre propiedad intelectual y derechos sociales y económicos, en particular con los derechos a la salud, alimentación, y acceso al conocimiento. Por el contrario, la observancia de la propiedad intelectual en sí misma ha sido un área relativamente descuidada, siendo el Acuerdo Comercial contra la Falsificación (ACTA) probablemente la única excepción

La observancia de la propiedad intelectual engloba una nueva generación de temas de reciente desarrollo normativo internacional, novedad que seguramente explica la embrionaria atención a las implicaciones en materia de derechos humanos en el plano global. La relación entre las normas relativas a la observancia de la propiedad intelectual y las normas sobre derechos humanos plantea *a priori* problemas en áreas adicionales a la del acceso a productos, aspecto que ha atraído la mayor parte de atención de la doctrina e instituciones internacionales.

1.2. Derechos humanos relacionados con la observancia

Las obligaciones en materia de observancia versan sobre cuestiones técnicas, aparentemente desprovistas de orientación axiológica. El derecho de los derechos humanos se ha desarrollado en cambio para proteger bienes jurídicos fundamentales estrechamente relacionados con valores. Por ello, el derecho internacional de los derechos humanos orienta y limita la protección de la propiedad intelectual,[1] y conmina a realizar las modulaciones precisas en los casos en los que existe tensión entre uno y otro régimen.[2]

Hasta la fecha la atención y análisis se han centrado en el impacto de la observancia sobre los derechos civiles. Existe una relación estrecha, prácticamente inherente, entre observancia y los derechos al acceso a un tribunal y a un juicio justo, puesto que las normas sobre observancia identifican el órgano que dirime las controversias y las normas que dicho órgano va a aplicar. Por otro lado, el poder de exclusión que caracteriza los derechos de propiedad intelectual, y que se materializa precisamente a través de las normas sobre observancia, explica el potencial impacto sobre la libertad de expresión y el derecho a la privacidad.[3]

La tradicional atención a las relaciones entre observancia y derechos civiles se ha complementado por el interés en torno a la relación entre la primera y diversos derechos

---

1 DRAHOS, P. (1999) «The universality of intellectual property rights: origins and development». En: WIPO, *Intellectual property rights and human rights*. Geneva: WIPO, p. 32.

2 SEUBA, X. (2008). «Intellectual property rights and human rights». En: CORREA, C.; YUSUF A. (Dirs.). *Intellectual Property And International Trade: Trips Agreement*. Dordrecht: Kluwer International Law. pp. 387-419.

3 *Vid*. MATULIONYTE, R. (2012). «ACTA' s Digital Chapter: remaining concerns and what can be done». *Queen Mary Journal of Intellectual Property*. Vol. 1, nº 3, pp. 248–271.

económicos, sociales y culturales. La regulación internacional en materia de observancia es cada vez más detallada, y de la misma resultan nuevos impactos económicos y efectos sobre el bienestar, y por ende afectaciones a derechos económicos y sociales. Debido a su papel decisivo a la hora de permitir la entrada de productos en el mercado, y afectar al comercio y la competencia, las normas sobre observancia pueden impactar por ejemplo sobre el acceso a la alimentación, a la cultura y a la salud.

Además del impacto directo sobre derechos pertenecientes a distintas generaciones de derechos humanos, las normas sobre observancia cumplen el que puede considerarse un rol instrumental, ya que permiten la materialización tanto de relaciones positivas como conflictivas entre propiedad intelectual y derechos humanos. Sin observancia, la discusión en torno a cuán conflictivas o positivas son las relaciones entre derechos humanos y propiedad intelectual no es más que un ejercicio teórico. Violaciones específicas de derechos humanos que tienen su origen en la regulación sustantiva de la propiedad intelectual se materializan a través de normas sobre la observancia de la propiedad intelectual. En sentido contrario, las normas sobre observancia pueden ser fundamentales para la satisfacción de varios derechos humanos, por ejemplo el derecho de los creadores e inventores a percibir los beneficios materiales y morales derivados de su obra.

Las normas sobre observancia están estrechamente relacionadas con derechos fundamentales de amplio alcance e impacto en la protección de otros derechos. Este es el caso de los derechos y principios relacionados con la administración de justicia, como el derecho a un recurso efectivo, el derecho a un juicio justo y el principio de legalidad. En estos casos las normas sobre observancia son el vehículo para garantizar tales derechos, que por otra parte son también instrumentos que permiten la protección de otros derechos fundamentales. Cuando un título de propiedad intelectual es o está a punto de ser infringido el derecho fundamental a la tutela judicial efectiva entra en liza. Por otra parte, numerosas normas relativas a la observancia determinan los derechos de las partes en el proceso, y permiten de este modo satisfacer el derecho a un juicio justo.

2. RELACIONES POSITIVAS

En este apartado se aborda la interacción entre el derecho a interponer un recurso y la observancia de la propiedad intelectual, con el fin de ilustrar relaciones sinérgicas entre observancia de la propiedad intelectual y derechos fundamentales.

El apartado 14.1 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) establece que toda persona tiene derecho a un juicio justo y público ante un tribunal competente, independiente e imparcial establecido por la ley. Asimismo, también prescribe que todas las personas deben gozar de igualdad ante los tribunales. El artículo 14 abarca el derecho de acceso a los tribunales en los casos de determinación de los derechos y obligaciones de carácter civil, así como la substanciación de acusaciones de carácter

penal, y establece las condiciones del debido proceso tanto en procedimientos judiciales como administrativos.

Las disposiciones en materia de observancia recogidas en tratados de propiedad intelectual identifican los recursos que permiten reaccionar frente a una violación de un derecho de propiedad intelectual y para que el presunto infractor pueda responder. Por lo tanto, las disposiciones sobre observancia ofrecen el cauce para que las partes ejerzan su derecho a un recurso efectivo. Dos artículos que se encuentran en numerosos tratados ilustran esta relación. Es frecuente que tratados internacionales sobre propiedad intelectual incluyan un artículo que obliga a las Partes a asegurar la existencia de «medidas, procedimientos y recursos» a su alcance, y que «permitan adoptar medidas eficaces contra cualquier acción infractora de los derechos de propiedad intelectual».[4] Otra disposición relevante y frecuente en tratados internacionales identifica quiénes son los «legitimados» en caso de infracción de un título de propiedad intelectual, es decir, determina la legitimación activa.[5]

Las características de los recursos judiciales destinados a garantizar el respeto de derechos fundamentales relacionados con las normas de propiedad intelectual han sido objeto de la atención de varios órganos internacionales de derechos humanos. En el caso del derecho de autores e inventores a gozar de los beneficios materiales y morales resultantes de sus obras e invenciones, las condiciones que deben cumplir los recursos judiciales son las mismas que las recogidas en importantes tratados de propiedad intelectual. El Comité de Derechos Económicos, Sociales y Culturales (Comité DESC) de Naciones Unidas ha señalado que «dichos recursos no deben ser excesivamente complicados o costosos, ni comportar plazos injustificables o retrasos innecesarios.»[6] Se trata exactamente de los mismos requisitos que se puede encontrar en el ADPIC y en diversos ACPs.[7]

El derecho a la tutela judicial incluye también los recursos adecuados de naturaleza administrativa, y requiere que sean accesibles, no onerosos, rápidos y eficaces.[8] Que el derecho a la tutela judicial puede implicar recursos administrativos es una precisión importante, puesto que en determinadas áreas la observancia de la propiedad intelectual –por ejemplo en las medidas de frontera– se materializa fundamentalmente a través de recursos administrativos, al menos en la fase inicial del procedimiento.

---

4 Acuerdo de Asociación entre la Unión Europea y Corea del Sur, Art. 10.41.2; Acuerdo de Libre Comercio entre Estados Unidos y Singapur, Art. 16.9.5.

5 *Vid*. por ejemplo Acuerdo entre la Unión Europea y Corea del Sur, Art. 10.42.

6 Committee on ESCR. (2005). *General Comment nº 17. The right of everyone to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he or she is the author (article 15, paragraph 1 (c), of the Covenant)*. par. 52.

7 *Vid*. Art. 151.2 de EU-CARIFORUM Association Agreement.

8 Committee on ESCR. (2005). *General Comment* nº 17. op. cit. pars. 43, 44, 45.

No todos los recursos judiciales relacionados con la observancia de la propiedad intelectual encuentran, sin embargo, justificación en argumentos de derechos humanos. Algunas de las iniciativas en el ámbito de la observancia penal han invocado la protección de derechos fundamentales como justificación subyacente a las mismas. En la Unión Europea éste ha sido el caso de la Directiva sobre observancia penal, la fallida IPRED2, que vinculaba su propia adopción a la satisfacción del artículo 17(2) de la Carta de los Derechos Fundamentales de la Unión Europea, que crípticamente anuncia que «Se protege la propiedad intelectual.»[9] Sin embargo, el Derecho internacional de los derechos humanos solamente obliga a adoptar medidas penales en reacción a las más graves violaciones de derechos humanos.[10] Parece, por tanto, que la referencia al artículo 17(2) de la Carta de los Derechos Fundamentales para justificar la adopción de la Directiva es un recurso retórico.

3. RELACIONES AMBIGUAS

3.1. Vaguedad y desequilibrio

La relación entre derechos humanos y normas de propiedad intelectual recogidas en tratados internacionales es más compleja que la de simple apoyo o conflicto. De hecho, las relaciones ambiguas entre uno y otro régimen son frecuentes. Dos características importantes de los nuevos compromisos internacionales en materia de observancia de la propiedad intelectual ponen de relieve la mencionada complejidad: la ambigua redacción de algunos artículos y el desequilibrio existente entre derechos de los titulares y derechos de terceros.

Los nuevos compromisos internacionales en materia de propiedad intelectual frecuentemente contienen disposiciones ambiguas, con obligaciones de significado incierto en materia de observancia. La inclusión de compromisos vagos y términos abiertos es parte de la que se ha venido a denominar «ambigüedad constructiva»,[11] que tiene por

9 *Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights*, {SEC(2005)848} /* COM/2005/0276 final-COD 2005/0127.

10 Este es el caso de la violación, castigo corporal a niños, homicidio violento y esclavitud. *Vid*. GRIFFITHS, J. (2012). «Criminal liability for intellectual property infringement in Europe: the role of fundamental rights». En: C. GEIGER (Ed.). *Criminal enforcement of intellectual property law*. Cheltenham: Edward Elgar. p. 198.

11 WATAL, J. (1999). «Intellectual Property Rights and Agriculture: Interests of Developing Countries». Paper presentado en *The Conference on Agriculture and the New Trade Agenda*. Geneva: World Bank, http://www.bvindecopi.gob.pe/colec/jwatal.pdf (visitada en noviembre de 2013).

objeto facilitar la conclusión del tratado a pesar de que existan diferentes puntos de vista sobre el significado y alcance de los artículos recogidos en el mismo.

La ambigüedad debe distinguirse de otra característica importante de los nuevos compromisos internacionales en materia de observancia, que es la creación de regímenes inequitativos donde normalmente los intereses de los titulares ocupan un lugar central, en ocasiones exclusivo. La inclusión de disposiciones inequitativas plantea varios problemas en términos de derechos humanos. En algunos casos, los problemas se relacionan con el impacto que un sistema inequitativo puede tener sobre diversos intereses sociales, como la alimentación, la salud o la competencia. En otras ocasiones, son los derechos civiles y políticos los que también se ven afectados por disposiciones en materia de observancia que no guardan el equilibrio necesario entre los derechos de los titulares y los derechos de terceros.

La ausencia de garantías procesales que protejan al presunto infractor hace que algunos artículos en materia de observancia recogidos en tratados internacionales sean especialmente preocupantes desde el punto de vista del respeto al derecho al debido proceso. En los acuerdos de asociación negociados por la Unión Europea, las disposiciones relativas a las medidas cautelares, mandamientos judiciales, derecho de información, pruebas y medidas para la preservación de pruebas no mencionan los derechos más elementales de los presuntos infractores.

3.2. Derecho al debido proceso e implementación de disposiciones internacionales en materia de observancia

Garantizado el derecho al acceso a un tribunal, la atención se desplaza a las características de los procedimientos a los que tal derecho abre la puerta. Las normas internacionales sobre el derecho al debido proceso y las garantías judiciales que le acompañan establecen un marco adecuado para evaluar normas de naturaleza procesal. Por ello, el derecho a un juicio imparcial es de sumo interés en el análisis de las normas sobre observancia de la propiedad intelectual, ya que éstas regulan específicamente los poderes y procedimientos disponibles para los titulares y los presuntos infractores.

Los principales convenios internacionales que regulan el derecho a un juicio justo aluden tanto a la 'substanciación de cualquier acusación de carácter penal'[12] como a la determinación de los 'derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter'.[13] El Comité de Derechos Humanos de Naciones Unidas ha aclarado a qué se refiere la determinación de derechos y obligaciones de 'carácter civil'. Según el Comité, la misma comprende a) procedimientos para determinar los derechos y las obligaciones

12 Art. 14.1 del Pacto Internacional de Derechos Civiles y Políticos.

13 Art. 8.1 Convención Americana de Derechos Humanos, Nov. 21, 1969; 1144 U.N.T.S. 143.

relativos a los contratos, la propiedad y los perjuicios extracontractuales en derecho privado, b) las nociones equivalentes de derecho administrativo, y puede comprender también (c) otros procedimientos que deberán evaluarse caso por caso.[14] Por su parte, el derecho a un juicio justo consagrado en el Convenio Europeo de Derechos Humanos es aplicable a las controversias entre partes privadas,[15] en materia contractual y responsabilidad civil, y se ha aplicado con eficacia a los litigios sobre propiedad intelectual.[16]

El derecho a un juicio justo tiene un amplio alcance, intensamente analizado y descrito por numerosos tribunales y organismos de derechos humanos. El Comité de Derechos Humanos ha hecho hincapié en la importancia que para el respeto al derecho a un juicio justo tienen los principios de igualdad de armas, procedimiento contradictorio, la prohibición de *reformatio in peius ex officio,* y la adopción de procedimientos expeditos.[17] En el contexto europeo el derecho a un juicio justo también se ha vinculado a los principios de igualdad de armas,[18] acceso efectivo a los tribunales[19] y participación efectiva en el proceso.[20] Muchos, si no todos, de estos requisitos son relevantes en el contexto de los litigios sobre propiedad intelectual. Por ejemplo, los órganos de derechos humanos han señalado que los procedimientos relacionados con determinados derechos de propiedad intelectual no deben ser 'excesivamente complicados o gravosos, ni comportar plazos injustificables o retrasos innecesarios'.[21]

3.3. El principio de igualdad de armas y las medidas de preservación de prueba

Preservar las pruebas sobre una presunta infracción es una medida importante para fomentar la eficiencia de los procedimientos de infracción de la propiedad intelectual. En Europa, la legislación armonizada relativa a las medidas para la preservación de pruebas

14 General Comment nº 32, par. 15.

15 VITKAUSKAS, D.; DIKOV G. (2012). *Protecting the right to a fair trial under the European Convention on Human Rights.* Strasbourg: Council of Europe, p. 14.

16 En *Nemec v. Slovakia* el Tribunal señaló que «the proceedings in issue concern a copyright. It is satisfied, and this was not contested by the parties, that the proceedings concern the determination of the applicants' «civil rights and obligations» within the meaning of Article 6 § 1.» ECHR, *Nemec v. Slovakia,* Application no. 48672/99, 2001, par. 29.

17 «the concept of a fair hearing in the context of article 14 (1) of the Covenant should be interpreted as requiring a number of conditions, such as equality of arms, respect for the principle of adversary proceedings, preclusion of *ex officio reformatio in pejus*, and expeditious procedure». *Yves Morael v. France*, Communication No. 207/1986, par. 9.3.

18 *Borgers v. Belgium* (1991) 15 EHHR 92.

19 *Golder v the United Kingdom* (1975) 1 EHRR 524.

20 *V v UK* (1999) 30 EHRR 121.

21 General Comment nº 17. op. cit. par. 52.

combina derechos tanto a favor del titular como del presunto infractor procedentes de las instituciones francesa 'saise de contrafaçon' y británica 'Anton Piller order'. Un análisis comparativo de las disposiciones sobre medidas de preservación de prueba que se recogen en los ACPs[22] permite identificar las garantías presentes en la legislación europea pero ausentes en tales acuerdos. Así, en los ACPs promovidos por la Unión Europea no se menciona la obligación de notificar inmediatamente después de la ejecución de la medida, el derecho (a ser escuchado y) pedir la revisión de la medida, el derecho a que las medidas sean revocadas si el procedimiento sobre el fondo no se inicia en un plazo razonable de tiempo, la posibilidad de solicitar una garantía suficiente o garantía equivalente, ni el derecho a ser indemnizado en caso de que las medidas sean revocadas o prescriban.

Si los artículos sobre preservación de pruebas se implementan tal y como están codificados en los tratados referidos, los titulares de derechos de propiedad intelectual sabrán que no se les requerirá indemnización alguna, inclusive en caso de que se determine que no ha existido infracción. También sabrán que el presunto infractor tendrá menos posibilidades de sostener sus argumentos y defender sus derechos en los tribunales. La fortalecida situación del titular debe ponerse en relación con el tipo de medidas autorizadas, que son altamente invasivas de la privacidad. En *Chappell c Reino Unido*, el Tribunal Europeo de Derechos Humanos trató una presunta violación del derecho a la intimidad derivada de la ejecución de una de las medidas sobre preservación de prueba antes mencionadas, una orden *Anton Piller*.[23] La Corte rechazó en última instancia la existencia de violación, pero hizo varias consideraciones de interés para el análisis de nuevas disposiciones sobre medidas para la preservación de pruebas.

El Tribunal centró su análisis sobre si la injerencia en el derecho a la privacidad había sido 'de conformidad con la ley' y 'necesaria en una sociedad democrática', dos criterios examiniados habitualmente por la Corte. La posibilidad de expedir una orden *Anton Piller* se encuentra en la ley británica, por lo que el Tribunal entendió que la exigencia de previsibilidad y accesibilidad se había satisfecho debidamente. Las observaciones del Tribunal fueron especialmente interesantes con respecto a la 'necesidad' de la orden. Fue en este contexto en el que el Tribunal se refirió a la existencia de garantías adecuadas, y sostuvo que 'es esencial que esta medida se acompañe de garantías adecuadas y efectivas contra injerencias arbitrarias y abusos'.[24] Por su parte, cuando previamente la Comisión de Derechos Humanos había indicado la aceptabilidad de la medida y aceptado la injerencia sobre el derecho a la intimidad, se refirió a la 'calidad de la ley' y a la compatibilidad 'con el imperio de la ley' de las medidas denunciadas.

22 Art. 238 del acuerdo con Perú y Colombia; Art. 10.44 del acuerdo con Corea del Sur; Art. 154 del Acuerdo Cariforum; Art. 263 del Acuerdo con América Central.

23 *Chappell v. United Kingdom* (1989) ECHR A 152 A.

24 *Ibid*. par. 57.

Componente básico del derecho al debido proceso, el principio de igualdad de armas implica que 'deben proporcionarse los mismos derechos procesales a todas las partes a menos que las distinciones se basen en la ley y puedan justificarse por motivos objetivos y razonables, sin implicar desventaja efectiva u otra injusticia para con el demandado'. Sin embargo, una serie de garantías importantes están ausentes en los nuevos compromisos internacionales en materia de observancia. En caso de que tales compromisos se implementen sin más en la legislación nacional se facilitarían las 'injerencias arbitrarias y abusos' que precisamente prohíbe el Tribunal.

Estas consideraciones sobre el marco jurídico para la aplicación de medidas para la preservación de pruebas permiten traer a colación algunas de las exigencias derivadas del derecho a un juicio justo. En su análisis de las órdenes *Anton Piller*, el Tribunal Europeo de Derechos Humanos ha subrayado la necesidad de proteger a los particulares frente injerencias arbitrarias y abusos, la prescriptiva calidad mínima de las normas y la compatibilidad de las medidas con el principio de legalidad. El frecuentemente inequitativo régimen internacional descrito en materia de observancia, recogido fundamentalmente en acuerdos comerciales, no cumple con el requisito de calidad ni ofrece tampoco garantías frente a injerencias arbitrarias.

4. RELACIONES CONFLICTIVAS

Tanto el ADPIC como los ACPs con disposiciones ADPIC *plus* y ADPIC *extra* han causado preocupación por su impacto sobre los derechos fundamentales. La relación entre ciertas categorías de propiedad intelectual con diversos derechos humanos ha llevado a afirmar la existencia de 'conflictos reales o potenciales' entre derechos humanos y propiedad intelectual,[25] algo que en materia de observancia se puede constatar en relación con el principio de seguridad jurídica.

El principio de legalidad prescribe la no retroactividad de las leyes y sanciones penales, y la necesidad de claridad, concisión y previsibilidad.[26] La seguridad jurídica 'expresa la premisa fundamental de que los que están sujetos a la ley debe saber cuál es la ley a fin de poder planificar sus acciones en consecuencia',[27] y se satisface cuando 'el individuo puede saber de la redacción de la disposición pertinente y, si es necesario,

25 UN Commission on HR, Sub-Commission on the Promotion and Protection of Human Rights, «Intellectual Property Rights and Human Rights», Fifty-second session, Agenda item 4, E/CN.4/Sub.2/2000/7, 17 August 2000.

26 KRESS, C. (2010). «Nulla poena nullum crime sine lege», *Max Plank Encyclopedia of Public International Law,* para. 29-31, http://www.uni-koeln.de/jur-fak/kress/NullumCrimen24082010.pdf (visitada en julio de 2013).

27 TRIDIMAS, T. (1999). *The General Principles of EC Law*. Oxford: Oxford, p. 163.

con la ayuda de la interpretación de la misma por parte de los tribunales, qué actos y omisiones desencadenan su responsabilidad.'[28] Algunas disposiciones sobre observancia penal recogidas en acuerdos bilaterales pueden violar el principio de seguridad jurídica en su vertiente de *lex certa.*

Varios ACPs establecen sanciones penales en respuesta a actividades elusivas de medidas tecnológicas de protección. Tales sanciones se aplicarán 'cuando se compruebe que cualquier persona, que no sea una biblioteca, archivo, institución educativa u organismo público de radiodifusión no comercial, se ha involucrado dolosamente y con el fin de obtener una ventaja comercial o ganancia económica privada en cualquiera de las actividades mencionadas'.[29] La referencia a la 'ganancia económica privada' como referencia para aplicar las sanciones penales se encuentra también en el marco de las disposiciones relativas a la información sobre la gestión de derechos.[30]

Del mismo modo, y de modo similar a como se ha señalado con respecto a ACTA,[31] varios ACPs promovidos por Estados Unidos obligan a establecer sanciones penales en los casos dolosos de piratería y falsificación a escala comercial. En el caso de los derechos de autor, 'escala comercial' comprende 'las infracciones significativas y deliberadas con fines de obtener una ventaja comercial o ganancia económica privada', así como 'la infracción dolosa que no tenga una motivación directa o indirecta de ganancia económica, siempre que haya un perjuicio económico superior a '*de minimis*'.[32] En otros tratados se establece que las 'violaciones dolosas significativas de derechos de autor y derechos conexos que no tienen motivación directa o indirecta en la obtención de un beneficio económico',[33] también dan lugar a sanciones penales, y no se menciona el requisito de que el perjuicio sea superior a '*de minimis*'. Por lo tanto, en un caso, se requiere la existencia de 'violaciones dolosas significativas' mientras en el otro caso es suficiente que exista 'más que un perjuicio económico 'de minimis".

La interpretación de estas disposiciones no es para nada clara. Por ejemplo, ¿Qué significa 'ganancia económica privada'? ¿Significa generar ingresos o basta con ahor-

28 ECHR, *Kokkinakis v Greece,* application no. 14307/88, 1993, para. 52.

29 Acuerdo de Libre Comercio entre Estados Unidos y República de Corea Art. 18.4. 7(a) 2 (ii); Acuerdo de Libre Comercio entre Estados Unidos y CAFTA-DR Art. 15.5. 7(a) 2 (ii); Acuerdo de Libre Comercio entre Estados Unidos y Australia Art. 17.4.7.

30 Acuerdo de Libre Comercio entre Estados Unidos y República de Corea Art. 18.4. 8(a).

31 GEIGER, C. (2014) «The Anti-Counterfeiting Trade Agreement (ACTA) and beyond: towards a differentiated approach to criminal enforcement of intellectual property rights at the global level», En: ROFFE, P., SEUBA, X. (Eds.). *The Plurilateral Enforcement Agenda: The Genesis and Aftermath of ACTA*. Cambridge: Cambridge University Press.

32 Acuerdo de Libre Comercio entre Estados Unidos y CAFTA-DR Art. 15.11.26(a).

33 Acuerdo de Libre Comercio entre Estados Unidos y República de Corea Art. 18.10. 26.

rar? ¿Cuáles son las *infracciones dolosas* 'significativas'? ¿En qué momento una infracción empieza a ser 'significativa' a los efectos de las sanciones penales? En ninguna parte se define qué es un perjuicio económico superior a 'de minimis'. En caso de que el acuerdo fuera de aplicación directa, ¿Qué criterios deberían seguir los jueces? Por último, ¿Qué significa exactamente 'motivación indirecta de ganancia económica'?

A la luz de las dudas existentes difícilmente se satisface el 'deber de los legisladores para que quede claro qué conducta dará lugar a las sanciones y a la privación de la libertad'.[34] La 'definición amplia' de un delito puede afectar negativamente a los derechos fundamentales, incluidos los derechos de naturaleza inderogable.[35] De acuerdo con el mismo Comité, la vaguedad de las definiciones es contraria al principio de legalidad,[36] particularmente el caso de la «redacción ambigua de las disposiciones y el uso de varias presunciones probatorias en detrimento del acusado».[37]

5. CÓMO ABORDAR LAS RELACIONES AMBIGUAS Y CONFLICTIVAS

5.1. La relevancia de las normas sobre interpretación de tratados

El derecho internacional general recoge un importante conjunto de normas secundarias para abordar las relaciones entre tratados. El punto de partida es premisa de la presunción en contra de la existencia de conflictos y el mandato de cumplir de buena fe los compromisos internacionales. En consecuencia, las relaciones ambiguas entre normas de propiedad intelectual y normas de derechos humanos deben abordarse a través de la interpretación y permitir, en la medida de lo posible, la aplicación de ambas normas.

Las técnicas hermenéuticas específicas para llevar a cabo esta operación se encuentran en la Convención de Viena sobre el Derecho de los Tratados (Convención de Viena). En su artículo 31 se recoge la 'norma general de interpretación' de los tratados, que prescribe una única operación conjunta basada en la interpretación textual, teleológica y contextual. El principio de integración sistémica, que recoge el artículo 31.3.c), forma parte de esta operación[38] e instruye tomar en consideración el conjunto de obligaciones internacionales

34 Irish Law Reform Commission, *Aggravated, Exemplary and Restitutionary Damages*, 1997, p. 99.

35 Estonia, ICCPR, A/58/40 vol. I (2003) 41 at par. 79(8).

36 Por ejemplo, «actividad extremista» ha sido considerada demasiada ambigua desde la óptica del principio de legalidad. Russian Federation, ICCPR, A/59/40 vol. I (2003) 20 en para. 64(20); *vid*, de forma similar, Marruecos, ICCPR, A/60/40 vol. I (2004) 35, par. 84(20).

37 Israel, ICCPR, A/58/40 vol. I (2003) 64 en par. 85(14).

38 MCLACHLAN, C. (2005) «The Principle of Systemic Integration and Article 31(1)(c) of the Vienna Convention», *International and Comparative Law Quarterly*. Vol. 54, nº 2, pp. 279 – 320.

existentes entre la partes a la hora de abordar la interpretación de una norma. De este modo, a la hora de interpretar el significado de una norma de la propiedad intelectual contenida en un tratado bilateral, otras normas, por ejemplo consagradas en una convención de derechos humanos, pueden ser tomadas en consideración.[39]

Como fuera señalado, el régimen sobre medidas para la obtención de prueba recogido en algunos ACPs resulta insatisfactorio desde el punto de vista del derecho de los derechos humanos. No obstante, el marco normativo de los ACPs puede mejorarse en la fase de implementación interna, tanto a través de la interpretación como de la adopción de legislación complementaria. Un buen punto de partida para ambas operaciones son las normas internacionales sobre el derecho a un juicio justo. Las garantías prescritas por este derecho deberán por tanto incorporarse en la legislación que se adopte para implementar los compromisos internacionales en materia de observancia.

5.2. Conflicto de tratados

Habrá casos en los que la conciliación propuesta no es posible y la relación derechos humanos y propiedad intelectual sólo puede abordarse a luz de las normas sobre conflicto de tratados. El artículo 30 de la Convención de Viena establece las normas básicas relativas a la aplicación de tratados sucesivos que sobre una misma materia, contempla la posibilidad de que los propios tratados incorporen cláusulas de conflicto, y codifica también el criterio cronológico siempre que las Partes en los tratados en conflicto coincidan. Sin embargo, cuando las Partes no coinciden enteramente la situación se torna algo más complicada. En este caso, la regla *lex posterior* se aplica entre las Partes que coinciden en ambos tratados (30.4.a), pero para el resto de Estados se aplicará el tratado en el que ambos coinciden, con independencia del criterio temporal (30.4.b). Este marco se completa con la regla consuetudinaria *lex specialis*, que establece la primacía de la norma más específica.

Los conflictos en los que una de las normas pertenece al selecto grupo del *ius cogens* son los más fáciles de resolver, ya que éstas son las únicas normas de derecho internacional público de jerarquía superior al resto. En este caso se está ante *conflictos inherentes,* de los cuales se derivan los resultados más drásticos, específicamente la nulidad de la norma contradictoria y del propio tratado que la recoge. Sin embargo, los derechos humanos que se considera que pertenecen a dicho grupo son pocos: la prohibición de

39 Sobre la específica implementación de este principio en el contexto de la solución de diferencias de la OMC en el área de la propiedad intelectual, *vid*. HESTERMEYER, H. (2007). *Human Rights and the WTO. The Case of Patents and Access to Medicines.* Oxford: Oxford University Press; SEUBA, X. (2010). «Mainstreaming the TRIPS and human rights interactions». En: CORREA, C. (Ed.). *The TRIPS Agreement*, Cheltenham: Edward Elgar Publishing. pp. 204-208.

la tortura, de la esclavitud y de la discriminación racial.[40] Si bien es cierto que la protección de la propiedad intelectual puede afectar el contenido básico de varios derechos humanos, no cabe sostener una equiparación entre *ius cogens* y el contenido esencial de los derechos. La existencia de una norma imperativa de derecho internacional general requiere su aceptación y reconocimiento 'por la comunidad internacional de Estados en su conjunto',[41] un consenso que no existe en relación con el paralelismo entre *ius cogens* y el contenido esencial de los derechos humanos.

La aplicabilidad del artículo 30 de la Convención de Viena se ciñe a los tratados sucesivos que versan sobre la misma materia, por lo que es determinante el juicio sobre si una norma de propiedad intelectual y otra sobre derechos humanos se refieren a la 'misma materia'. Dos tratados se ocupan de la 'misma materia' si el cumplimiento de la obligación establecida en un tratado afecta al cumplimiento de una obligación establecida en otro tratado.[42] Por lo tanto, se satisface dicha relación siempre que sea posible demostrar que el cumplimiento de una obligación establecida en un tratado de propiedad intelectual afecta el cumplimiento de la obligación establecida en un tratado sobre derechos humanos.

Cuáles sean los Estados Parte de los tratados en conflicto y la fecha de ratificación de los mismos determinará la norma aplicable a la controversia. El artículo 30 de la Convención de Viena resulta en principio claro: si ambos estados coinciden en los tratados afectados, prevalecerá el último tratado, pero si los Estados no coinciden será de aplicación solamente aquel convenio en el que efectivamente coincidan. En la práctica, esto parecería indicar que en la mayoría de los casos los tratados de propiedad intelectual prevalecerán sobre las disposiciones contenidas en tratados de derechos humanos, puesto que son más recientes y además algunos de los promotores de los tratados de propiedad intelectual (en particular los Estados Unidos) no son miembros de los tratados de derechos humanos con los que se detecta el conflicto.

El debate más importante sin embargo es el relativo a la aplicación de las normas sobre conflicto de tratados a tratados de derechos humanos. Es ampliamente aceptado que los tratados de derechos humanos tienen características especiales que excluyen la aplicación de una serie de normas de derecho internacional general. Su carácter objetivo, la especialidad del régimen de reservas, el debate en torno a su relación con el *ius cogens*, y

40 International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of Its Fifty-third Session*, UN GAOR, 56th Sess. Supp. nº 10, UN Doc. A/56/10 (2001), pp.202, 282-284.

41 Art. 53 de la Convención de Viena.

42 International Law Commission, *Fragmentation of international law: difficulties arising from the diversification and expansion of international law, report of the Study Group of the International Law Commission*, A/CN.4/L.682, 13 April 2006, p. 130.

la calificación de los derechos humanos como obligaciones *erga omnes*, apuntan hacia la relación especial que existe entre derecho internacional de los derechos humanos y derecho internacional público. Un tratado de derechos humanos es un tratado *absoluto* o *integral,* distinto de los que se establecen las obligaciones sinalagmáticas o interdependientes. Un Estado no puede violar un tratado de derechos humanos solamente con respecto a una de las Partes mientras continúa con su aplicación con respecto a las otras. Las Partes de un tratado de derechos humanos deben salvaguardar los derechos de las personas bajo su jurisdicción, algo que no es posible satisfacer parcialmente. Debido a la naturaleza integral de los tratados de derechos humanos, y la naturaleza *erga omnes* de las obligaciones establecidas en el mismo, el incumplimiento sería de tal naturaleza que cambiaría radicalmente la situación de todos los otros Estados con los cuales se ha contraído la obligación.

La Comisión de Derecho Internacional ha afirmado que las obligaciones integrales, y más concretamente las obligaciones de derechos humanos, gozan de cierta prioridad en relación con los instrumentos meramente transaccionales. Las técnicas 'ordinarias' utilizadas para abordar la relación entre tratados bilaterales sinalagmáticos no se ajustan a la naturaleza y contenido de los tratados de derechos humanos. Las consecuencias de la violación de obligaciones *erga omnes* y normas integrales son particularmente graves: no se podrán invocar las normas que causan tal violación y el resto de Estados parte en la convención está obligado a no reconocer la situación resultante.[43] En el preciso ámbito de interés que nos ocupa, esto llevaría a concluir la inaplicación de las obligaciones en materia de observancia cada vez que entran en conflicto con las normas de derechos humanos.

Se trata de un resultado drástico, y que ilustra que las normas de derecho internacional general sobre conflicto de tratados no abordan adecuadamente la complejidad de las interacciones entre regímenes internacionales. A nuestro juicio, se trata de un resultado sostenible en lo académico pero difícilmente en la realidad de las relaciones internacionales. Sin embargo, también es posible sostener que la comunidad internacional reconoce prioridad a las normas de derechos humanos y los resultados mencionados anteriormente son en realidad los deseados. El principio *pro homine* inherente al régimen internacional de derechos humanos, y la identificación de la dignidad humana como un interés jurídico fundamental protegido por el sistema jurídico internacional en su conjunto, dan crédito a esta última opinión.

6. CONCLUSIÓN

A través del estudio de la codificación internacional del derecho a un recurso, las medidas de preservación de prueba y las sanciones penales en caso de infracción de de-

43 *Vid.* por ejemplo *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ Reports 2004,* par. 159.

rechos de propiedad intelectual se ha propuesto una primera aproximación sistemática a las relaciones positivas, ambiguas y conflictivas entre derechos humanos y observancia de la propiedad intelectual, así como también a las normas internacionales que detallan cómo abordar este tipo de relaciones. Se trata de un ámbito prácticamente inexplorado por la doctrina y la jurisprudencia internacional, descuido que, a la luz de la gran proliferación de normativa internacional referida a la observancia de la propiedad intelectual merecería, muy probablemente, ser corregido.

7. BIBLIOGRAFÍA

Drahos, P. (1999). «The universality of intellectual property rights: origins and development». En: WIPO, *Intellectual property rights and human rights.* Geneva: WIPO. En: http://www.wipo.int/edocs/mdocs/tk/en/wipo_unhchr_ip_pnl_98/wipo_unhchr_ip_pnl_98_1.pdf (visitada Agosto 2013).

Dreier, T. (1996). «TRIPS and the Enforcement of Intellectual Property Rights». En: BEIER, F. K., Schreiker, G. (Eds.). *From GATT to TRIPs: the Agreement on Trade-Related Aspects of Intellectual Property Rights*. Weinheim: VCH. pp. 248-277.

Geiger, C. (2012). «The Anti-Counterfeiting Trade Agreement and Criminal Enforcement of Intellectual Property: What Consequences for the European Union?». En: ROSEN, J. (ed.). *IP Rights at the Crossroads of Trad*e. Cheltenham: Edward Elgar, 2012.

Geiger, C. ; D'Erme, R.; Grosse-Ruse Kahn, H.; Heinze, C.; Jaeger, T.; Matulionyte, R.; Metzger, A. (2013). «The Impact of the Anti-Counterfeiting Trade Agreement on the Legal Framework for IP Enforcement in the European Union». En: Geiger, C. (Ed.). *Constructing European Intellectual Property: Achievements and New Perspectives,* Cheltenham: Edward Elgar, pp. 394-408.

Geiger, C. (2014). «The Anti-Counterfeiting Trade Agreement (ACTA) and beyond: towards a differentiated approach to criminal enforcement of intellectual property rights at the global level». En: Roffe, P., Seuba, X. (Eds.). *The Plurilateral Enforcement Agenda: The Genesis and Aftermath of ACTA*. Cambridge: Cambridge University Press.

Griffiths, J.; Suthersanen U. (Eds.) (2005), *Copyright and Free Speech: Comparative and International Analyses*. Oxford: Oxford University Press, p. 287.

Griffiths, J. (2012). «Criminal liability for intellectual property infringement in Europe: the role of fundamental rights». En: GEIGER, C. (Ed.). *Criminal enforcement of intellectual property law*, Cheltenham: Edward Elgar, pp. 198-212.

Haveman, R. (2003). «The Principle of Legality». En: Haveman, R.; Kavran, O.; Nicholls J. N. (Eds.). *Supernational Criminal Law: A system sui generis*. Antwerp-Oxford-New York: Intersentia, pp. 39- 40.

Lamb, S. «Nullum Crimen, Nulla Poena Sine Lege in International Criminal Law». En: Cassese, A.; Gaeta, P.; Jones J. R. W. D. (Eds.), *The Rome Statute of the International Criminal Court: A commentary*. Oxford: Oxford University Press. 2002. pp. 733-774.

Hestermeyer, H. (2007). *Human Rights and the WTO. The Case of Patents and Access to Medicines.* Oxford: Oxford University Press.

Lemley, M.; Volokh, E. (1998). «Freedom of speech and injunctions in intellectual property cases». *Duke Law Journal*. Vol. 48, p. 147.

Kress, C. (2010). «Nulla poena nullum crime sine lege», *Max Plank Encyclopedia of Public International Law,* Oxford: Oxford University Press. para. 29-31, http://www.uni-koeln.de/jur-fak/kress/NullumCrimen24082010.pdf (visitada en julio de 2013).

Korff, D.; Brown, I. (2011). «Opinion on the compatibility of the Anti-Counterfeiting Trade Agreement (ACTA) with the European Convention on Human Rights & the EU Charter of Fundamental Rights». En: http://rfc.act-on-acta.eu/fundamental-rights (visitada en Julio 2013).

Mclachlan, C. (2005). «The Principle of Systemic Integration and Article 31(1)(c) of the Vienna Convention», *International and Comparative Law Quarterly.* Vol. 54, nº 2, pp. 279 – 320.

Pauwelyn, J. (2003). *Conflict of Norms in Public International Law. How WTO Law Relates to Other Rules of International Law*. Cambridge: Cambridge University Press.

Roucounas, E. (1987). *Engagements Parallèles et Contradictoires. Recueil des Cours.* Vol. 206.

Seuba, X. (2008). «Intellectual property rights and human rights». En: Correa, C.; Yusuf A. (Dirs.). *Intellectual Property And International Trade: Trips Agreement.* Dordrecht: Kluwer International Law. pp. 387-419.

Seuba, X. (2010). «Mainstreaming the TRIPS and human rights interactions». En: Correa, C. (Ed.). *The TRIPS Agreement*, Cheltenham: Edward Elgar Publishing, pp. 192-215.

Seuba, X. (2013). «Checks and balances in the intellectual property enforcement field: reconstructing EU trade agreements». En Geiger, C. (Dir*). Constructing European IP: Achievements and News Perspectives.* Cheltenham: Edward Elgar Publishing, pp. 409-431.

Torremans, P. (Ed.). *Intellectual Property and Human Rights: Enhanced Edition of Copyright and Human Rights*». Dordrecht: Kluwer Law International, pp. 131-155.

Vitkauskas, D., Dikov G. (2012). *Protecting the right to a fair trial under the European Convention on Human Rights.* Strasbourg: Council of Europe .

Yu, P. K. (2010). «The Graduated Response». *Florida Law Review.* Vol. 62, pp. 1373-1430.

2

DON'T THINK TWICE, IT'S ALL RIGHT: TOWARDS A NEW COPYRIGHT PROTECTION SYSTEM

Pedro Letai
Professor of IE Law School [1]

ABSTRACT: Legal scholars and economists often debate in the literature about current terms of copyright protection. Those terms seem unwarranted and disproportionate, leading to a market failure on the effective life of works. The de lege ferenda proposal which is here formulated, based on a simple system of short and renewable protection periods, finds serious benefits from both economic and social perspective.

Major parts of our cultural heritage have been digitalized, but are not accessible on line to the general public because of excessive copyright protection. The effective exploitable life of the vast majority of artistic creations is brief, and the question that arises is how can we turn that deadweight loss into profit, with incentive for creators and the least social cost. It then seems logical that after the above mentioned period of exploitation works should enter the public domain. Furthermore, the proposed system provides greater protection to the original authors besides eventual intermediaries as rights holders, with a revertible formula which may strength their position at the time of negotiating over the ownership of their works.

With the technological advances of the digital age, economic analysis of copyright should no longer be concerned on incentivizing creation, which in itself is already unstoppable, but to facilitate the dissemination of works. That contents' diffusion would be hugely advantageous for the society and, moreover, for the copyright holders who, ideally, should remain the authors themselves.

KEYWORDS: Copyright; Intellectual Property; Law & Economics, Policy, Behavioral Economics.

---

1 Professor of Law, IE Law School. LL.B. 2005, Universidad Autónoma de Madrid; LL.M. 2007, IE Law School; Ph.D. 2012, Universidad Autónoma de Madrid. I am grateful to my colleagues Peter C. DiCola (Northwestern Law), Fernando Gómez Pomar (Universidad Pompeu Fabra), Emanuela Carbonara (Università di Bologna), Francisco Marcos (IE Law School), Jesús Alfaro (Universidad Autónoma de Madrid), and to seminar audiences at Harvard Law School (X Seminar on Law & Economics) and Italian Society of Law and Economics (Lugano, 2013) for their advice and comments. I wish to thank my fellow researcher Martyna Polak for her great effort and commitment. The views expressed in this article are however my own, and my responsibility. Research grants came from IE Law School and Northwestern University; my great thanks to Deans De Cendra and Rodriguez, and very special to Tim Jacobs for his kindness and help in Chicago. All my gratitude to my admired friend Fred McChesney.

1. INTRODUCTION

No author, artist or production company invests creativity or resources with a view of recoupment in 50 or 100 years. To encourage creativity, copyright creates intellectual property rights for original works of authorship in literature and music, computer software, web content and many other important sectors of the digital economy. Extensions in the length of copyright have emerged as a key policy lever by which national governments attempt to strengthen property rights in expressed ideas. For example, the U.S. Copyright Act of 1998 and the U.K. Copyright Act of 2011 extended the length of copyright protection for music from 'life of author plus 50 years' to 'life of author plus 70 years'. Proponents of longer copyright argue that such shifts encourage creativity by increasing expected profits from works. Systematic evidence on the effects of stronger copyrights on the profitability of authors, however, is scarce because data on payments to authors is typically not available to the public.

There are number of costs to granting overbroad intellectual property rights. First, intellectual property rights distort markets away from the competitive norm, and therefore create static inefficiencies in the form of deadweight losses. Second, intellectual property rights interfere with the ability of others creators to work, and therefore create dynamic inefficiencies. Third, the prospect of intellectual property rights encourages rent-seeking behavior that is socially wasteful. Finally, overinvestment in research and development is in itself a distortion. The ultimate result of these costs is that what we want is not a mere incentive but the right incentive.[2]

Although it seems difficult to draw the right economic line on copyright law, we can take some minimum guidance from the likelihood that the relationship between intellectual property protection and innovation is not monotonic. Because of the above mentioned costs, adding more and more intellectual property protection not only has diminishing marginal benefits, but at some point has a net negative impact on innovation, because the strengthening of existing rights stifles more new innovation building on those rights than further expansion encourages.

At a bare minimum, increases in intellectual property protection that restrict more innovation than they encourage cannot be economically justified.[3] An obvious example is the retroactive extension of copyright term in the Sonny Bono Copyright Term Exten-

2 Lemley, Mark A., Property, Intellectual Property and Free Riding, *Texas Law Review*, Vol. 83, p. 1031, 2005.

3 Wagner, R. Polk, Information Wants to be Free: Intellectual Property and the Mythologies of Control, 103 *Columbia Law Review* 995 (2003). Wagner argues that since control over intellectual property is imperfect, increasing intellectual property rights will encourage new creation that will have spillover benefits to the public. While this is certainly true up to a point, beyond a certain level of control the costs of marginal increases in control outweight any such benefits.

sion Act[4], which provided no new incentive to authors and complicated efforts to make use of a large number of existing works.[5] With that policy tendency we are at danger of ending on a system of perpetual protection. This paper tries to combat that drift with a simple proposal bias economic efficiency.

2. REVIEWING THE POLICY AND ECONOMICS OF COPYRIGHT PROTECTION: FROM INCENTIVIZE TO DISSEMINATE

Copyright protection, that is the right of copyright's owner to prevent others from making unauthorized copies, trades off the costs of limiting access to a work against the benefits of providing incentives to create the work in the first place. Striking the correct balance between access and incentives is the central problem in copyright law but, as polar opposites-attract, perhaps the best option would be that of incentivizing access in a way that ends to be beneficial also to the authors. For copyright law to promote economic efficiency its principal legal doctrines must, at least approximately, maximize the benefits from creating additional works minus both the losses from limiting access and the costs of administering copyright protection.[6]

The incentive theory of copyright aims to provide incentives to two kinds of actors in the economy: creators and intermediaries. Copyright law grants certain exclusive rights to creators of original works that are fixed in a tangible medium of expression.[7] If we take the music industry as a case study, this means both compositions and sound recordings, which are separate types of copyrightable subject matter. Creators may, of course, release their own works to the public, but in practice the copyright system is designed with the expectation that many creators will contract with intermediaries to exploit their works commercially.[8]

Wagner simply assumes we haven't reached that point. We think there is substantial evidence to the contrary in copyright law.

4 17 U.S.C. 302.

5 For an economic critique of the Act, see Eldred v. Ashcroft, 537 U.S. 186, 242 (2003) (Breyer, J., dissenting).

6 Landes, William M. and Posner, Richard A., An Economic Analysis of Copyright Law, *The Journal of Legal Studies*, Vol. 18, No. 2 (Jun., 1989), p. 326 *et seq*.

7 DiCola, Peter C., Money from Music: Survey Evidence on Musicians Revenue and Lessons About Copyright Incentives (January 9, 2013). *Arizona Law Review*; Northwestern Law & Econ Research Paper No. 13-01.

8 Litman, Jessica, Real Copyright Reform, 96 *Iowa L. Rev.* 1, 10-12 (2010), explains how copyright law contemplates that creators will transfer their copyrights to intermediary distributors.

Intermediaries offer the prospect of capital investment, marketing, promotion, and wider distribution, which together generate larger financial rewards than the creator could collect on his own. In return, the creator must transfer either copyright ownership or a large royalty share to the intermediary. For example, in the music industry, recording artists typically transfer their sound recording copyrights to record labels in return for royalties.[9] Composers and songwriters typically sell or license their composition copyrights to publishing companies, which will administer the copyright in return for a percentage of the proceeds. Thus, intermediaries often own the copyrights and receive a medium to large share of the proceeds from exploiting the works, the creators receive royalties and the listening public benefits from the works that reach them.

2.1. The Classic Economic Approach to Copyright Protection: The Incentive Theory

The incentive theory contemplates a chain of value, as outlined above, from creator to distributor to the listening public. It also contemplates money flowing in the opposite direction, from the consumers to distributors to creators, so we'll have to take into account very seriously the nature of the financial rewards that authors receive from their works in order to assess whether particular changes to copyright legislation would encourage more creative activity or, if so, how much more.

It has been well established in the economic literature that copyright is a trade-off between opposing forces –the economic incentive to create works of art, literature, music, etc. as against the disincentive it causes to users, whether intermediate producers or final consumers. It is a second best solution to market failure and there is no best answer; all we can do is to aim for features of the law that maximize net benefits and deal with externalities. In common with other second best situations facing policy-makers, empirical evidence on costs and benefits is needed to establish these net benefits in specific cases as there is no general answer.

The so-called 'copyright standard' consists of the duration of the term of its many rights and their scope as well as the degree to which it is enforced. Almost all economists are agreed that the copyright term is now inefficiently long with the result that costs of compliance most likely exceed any financial benefits from extensions. At this initial point it is worth remembering that the term of protection for a work in the 1709 Statute of Anne was 14 years with the possibility of renewal as compared to 70 years plus life for authors in most developed countries in the present, which means

9 *See* Kembrew, McLeod and DiCola, Peter, *Creative License; The Law and Culture of Digital Sampling* 76, 79-82 (2011) summarizing the role of record labels in the music industry and their contractual relationship with recording artists.

a work could be protected for well over 150 years. Moreover, difficulties of tracing copyright owners and orphan works has prevented access to copyright material and inhibited both future creation and access to culturally valuable material by the public. It is well known that the vast majority of copyright works is out of print or has long been unavailable on the market and this tendency is exacerbated by extending the term.[10] One point on which economists agree is that there can be no possible justification for retrospective extension to the term of copyright for existing works since it defies the economic logic of the copyright incentive, which nevertheless has been enacted on several occasions.[11]

In addition, the scope of copyright is very broad and nowadays covers many items of no commercial value that were never intended to be commercialized, as is the case with a great deal of material on social networking sites. This raises the question of the incentive role of the scope of copyright since it offers the same coverage for every type of qualifying work. In general, the lack of discrimination in this 'one size fits all' aspect of copyright is another subject on which economists are agreed: in principle, the incentive should fit the type of work depending upon the investment required, the potential durability of the work and other heterogeneous characteristics. This applies as much to the term as to the scope of copyright; only few works retain their value over a very long period while most of them lose it very quickly. The rationale for this lack of discrimination, however, is that individualizing incentives would be prohibitively costly both to initiate and to enforce. As it is, that copyright is recognized to have become excessively complex and therefore very costly for users and authors.

A further aspect of the incentive value of copyright has to do with practicalities. Copyright law only stipulates the copyright standard and the rights that protect authors, but authors almost always have to contract with an intermediary or distributor in order to market their work and it is the terms of the contract between them that determine the eventual financial reward to the author. That outcome is uncertain, though, as the contract usually only lays down the royalty rate, not the value of the revenue of which it is a percentage. For many rights, such as the public performance right, individual authors and performers cannot contract with all users and the solution is through collective rights management. That minimizes transaction costs for both copyright holders and users of copyright material but introduces monopoly pricing and blunts the individual incentive, which is actually another trade off. Technical alternatives, such as digital rights management that are supposed to enable individual control, even if fea-

10 Breyer, S., The Uneasy Case for Copyright: A Study of Books, Photocopies and Computer Programs, *Harvard Law Review*, 84; 281-351 (1970).

11 Perhaps the most notorious case was the CTEA (*Sonny Bono* or *Mickey Mouse*) extension in the USA, which was also followed up by the European Union, thereby handing out economic rents to the *rich and famous* of the entertainment world and, more likely, to their descendants.

sible, do not solve the problem of setting the royalty rate. Most economists agree that collective rights management is necessary in those circumstances in order for copyright to be practicable.[12]

Economists have made some headway in estimating earnings from copyright, which is significant for the question of the importance of the incentive it offers to creators. Research on royalty earnings of individual creators and performers has been limited because by and large, it has been on earnings from specific rights rather than on the entire bundle: for example, we know what composers earn from performing and mechanical rights for their compositions but not what they earn from performers –rights as well, as players or conductors. Research on artists' total earnings including royalties shows that only a small minority earns an amount comparable to national earnings in other occupations and only superstars make huge amounts. Copyright produces limited economic rewards to the ordinary professional creator; on the other hand, what the situation would be like absent copyright protection cannot be estimated. There has also been recent work on estimating the asset value of original works of art to which copyright applies that is a notable set forward in the measurement of the economic contribution of the products embodying these copyright works but again, it does not tell us what incentive role copyright had in stimulating that production.[13]

In this context, it is generally accepted by economists that piracy has adversely affected sales in creative industries that did not anticipate effects of digitalization, P2P, MP3 and other such means of using the Internet to obtain unauthorized copied, especially in sound recording. We do not know the true size of the effect –how much of the loss in sales is actually due to piracy, and how much to other effects–, nor do we know the real cost to the industry –losses in profit rather than sales. Nor has there been research on the distribution of the loss of potential revenue to authors and performers.

Economists have responded to the apparent threat to copyright posed by digitalization by suggesting that copyright law is anyway excessively complex and unnecessary if suitable business models are developed that would enable the market alone to reward the owner. Some have gone further and argued that copyright inhibits the development

12 Towse, Ruth, What We Know, What We Don't Know, and What Policy-makers Would Like Us to Know About the Economics of Copyright (December 31, 2011). *Review of Economic Research on Copyright Issues*, Vol. 8, No. 2, pp. 101-120, 2011.

13 For the UK, *see* Farooqui, S., Goodrige, P. and Haskel, J., *The Role of Intellectual Property Rights in the UK Market Sector*, Newport, UK, Intellectual Property Office, 2011. For the US, Soloveichik, R., Artistic Originals as a Capital Asset, Working Paper for the Bureau of Economic Affairs, Washington DC; or Soloveichik, R. and Wasshausen, D., Copyright Protected Assets in the National Accounts, Washington DC, U.S. National Academies of Science.

of these models.[14] One solution to the difficulties of enforcing copyright in the digital age that has been widely adopted is the copyright levy, that has been almost universally opposed by economists on the grounds that its remuneration to creators bears no resemblance to the market value of the works and therefore could not act as a valid incentive to creators. Its only merit is that it reduces transaction costs of obtaining remuneration for right holders, though it is argued that it acts as a tax on goods, such as computers, that are not directly responsible for the uses or abuses to which they are put.

Finally, economists have had long concerns that copyright has a moral hazard effect on incumbent firms, including those in the creative industries, by encouraging them to rely on enforcement of the law rather than adopt new technologies and business models to deal with new technologies. Many economists espouse the Schumpeterian view of the process of creative destruction of technical progress, whereby incumbent firms are replaced by new firms / industries that have developed the ability to exploit new technologies.[15] It is well-known that creative industries have spent huge amounts of money lobbying governments for increased copyright protection both through strengthening the law and stronger enforcement, not only within national boundaries but also through international treaties.

2.2. The Unknown Optimal Scope and Duration of Copyright

Economics scholars have found it very difficult to provide empirical evidence on the impact of copyright as there are no obvious counter-factual, that is, situations comparable to those in which copyright does apply to one in which it does not. Given the widespread application of copyright, its impact cannot be distinguished. Copyright's scope is universal with the definition of the law. Even where copyright may not be regarded as useful in the production of some cultural goods or services, it still applies. For instance, few choreographers need to rely on enforcing copyright to protect their work as reputation will do the job but nevertheless, choreography falls within the scope of the law at it cannot be ruled out that copyright plays a role in stimulating creativity in dance. There is evidence from surveys of firms that some regard copyright as not only not useful

14 *See* Varian, H., Copying and Copyright, *Journal of Economic Perspectives*, 19(2), pp. 121-138 (2005); and Boldrin, M. and Levine, D., The Case against Intellectual Property, *The American Economic Review, 92(2), pp. 209-212* (2002).

15 Aghion, P. and Howitt, P., *Endogenous Growth Theory*, Cambridge, MA, MIT Press (1997); Metcalfe, S., Evolutionary Economics and Creative Destruction, *Graz Schumpeter Lectures*, 1, London, Routledge (1998). For relevance to the music industry *see* Liebowitz, S., File-Sharing Creative Destruction or just Plain Destruction?, *Journal of Law and Economics*, 49(1); pp. 1-28 (2006) and Handke, C., Plain Destruction or Creative Destruction? Copyright Erosion and the Evolution of the Record Industry, *Review of Economic Research on Copyright Issues*, 3(2); pp. 29-51 (2006).

to their enterprise but actually that it even imposes costs on some.[16] Moreover, economics does not deal easily with all or nothing states of the type envisaged by the impact of the whole system; its strength is in analyzing marginal changes.

Even if some feasible scenario can be found, the absence of registration of copyright works makes direct research on the effects of copyright impossible, unlike the position with patents. By direct research we mean where works can be identified and their exploitation trace through the market. As the requirement of compulsory registration of works contravenes the Berne Convention, signatories therefore have had to abandon registration if they require it prior to joining.[17] Consequently, researchers must use either old registrations or abandon the attempt to work with direct data in copyright works and substitute instead products that contain a strong element of copyright material, such books and sound recordings. That has been the most common approach to measuring the effect of the copyright incentive. The reasoning can be circular: the creative industries are mostly defined in terms of their reliance on copyright so cause and effects become confused.[18] Even where they measure value added to national economies by the creative industries, benefits are overestimated by omitting the balance of payments of royalties, for which data barely exist and of overseas transfer of profits by multi-national corporations which dominate the publishing, music and film industries, among others. Moreover, in cost benefit terms, these measures fall as they concentrate entirely on the supposed benefits but completely ignore the costs of copyright to users and consumers and the deadweight loss of administrative costs.

It has been argued that the advent of digitalization provides a natural experiment for researching the economic importance of copyright and that measuring the value of lost sales and other revenues due to unauthorized use of copyright works is evidence of the value of copyright. Experience with empirical testing of piracy has shown difficulties of this research[19] and although there is a consensus now that it has had a significant impact, particularly in sound recording as the industry most researched by economists,

16 *See* Handke, C., Plain Destruction or Creative Destruction? Copyright Erosion and the Evolution of the Record Industry, *Review of Economic Research on Copyright Issues*, 3(2); pp. 29-51 (2006).

17 Some interesting studies on this field can be seen in Khan, Z., Does Copyright Piracy Pay? The Effects of US International Copyright Laws on the Market for Books, 1790-1920, *NBER Working Paper* 10271 (2004); or Heald, P., Bestselling Musical Compositions (1913-32) and Their Use in Cinema (1968-2007), *Review of Economic Research on Copyright Issues*, 6(2); 31-60, (2009).

18 *See* Towse, R., Creativity, Copyright and the Creative Industries Paradigm, *Kyklos*, 3: pp. 483-500, (2010).

19 *See* Handke, C., The Economic Effects of Copyright: The Empirical Evidence So Far, *Report to National Academies*, Washington DC, (2011).

it has taken almost a decade for that consensus to emerge and during this time, not only has the technology changed, especially of distribution, but the players in the industry have changed too. This suggests how much more difficult it would be to measure a value for copyright in the whole economy.

The genius of the competitive market is precisely that while no individual producer has the incentive to fill market demand perfectly, collectively producers will meet that demand. This is not because they capture the full social surplus from their behavior, which by definition is never true in a competitive market. It is because they have enough incentive to produce what consumers demand. The reason we can generally rely on private ordering to produce desirable outcomes is not because property has some inherently moral virtue that leads to efficient conduct, nor because individual companies can eliminate free riding, but because individual companies are constrained by the discipline of a competitive market.[20]

2.3. Not Only to Encourage But to Spread: From Incentivize to Disseminate

Copyright law also presents another trade-off, this one not between authors and consumers, but between authors and other authors. It is a commonplace that new works draw from and build upon old ones.[21] No work is purely and completely new. All works draw upon prior works, to at least some extent. Thus, by increasing protection for initial works, we may increase the incentives for producing such works, but we also increase the cost of producing works that draw upon these initial works[22]. If protection is too great, we may in fact decrease the number of total works, that is, the sum of both original and follow-on works. If our aim is to provide adequate incentives for both initial and follow-on works, the strength of copyright protection needs to reflect this balance.[23]

The length of the copyright term is one way –among many ways– in which this balance is struck. Too short a term, and the incentives may not be sufficient to spur initial

20 *See* Lemley, Mark A., Ex Ante Versus Ex Post Justifications for Intellectual Property (February 2, 2011). University Chicago Law Review, Vol. 71, p. 129, 2004; UC Berkeley Public Law Research Paper No. 144.

21 *See* Goldstein, P., Derivative Rights and Derivative Works in Copyright, *30 J. Copyright Soc'y U.S.A.* 209, 218. (1983); or Jaszi, P., Toward a Theory of Copyright: The Metamorphosis of 'Authorship', *1991 Duke L.J.* 455, 457-63.

22 *See* Brief of George A. Akerlof et al. as Amici Curiae in Support of Petitioners, Eldred v. Ashcroft, 122 S. Ct. 1170 (2002). (no. 01-618), pp. 12-13; or Landes, W., and Posner, R., An Economic Analysis of Copyright Law, *18 J. Legal Stud.* 325, 333 (1989).

23 *See* Landes, W., and Posner, R., An Economic Analysis of Copyright Law*, 18 J. Legal Stud. 325, 333* (1989); or Netanel, N., Copyright and a Democratic Civil Society, *106 Yale L.J. 283*, p. 295. (1996).

creation, since authors may not have enough time to obtain sufficient compensation for their efforts. Too long a term, and the work may not be widely disseminated or built upon over time.[24]

Copyright seeks a diversity of expression. It is designed to permit variations, new expressions built upon existing ideas. We are not disturbed by the idea that anyone can make a movie re-telling, in any form, the story of Rome and Juliet or record a new interpretation of a Beethoven Symphony –indeed, this is generally seen as a good thing. At the same time, society's interest in seeing different perspectives and re-interpretations of the original works increases over time. Furthermore, copyright must do more to actively support an interest in the re-interpretation and fair use of copyrighted works. People must have some degree of freedom to play with intellectual goods, to re-cast them, to imbue them with meanings independent of the ones that the original author intended, in order to make sense of them. These transformative activities are an essential part of what it means to consume an intellectual good. The longer a work has been published, the more desirable it becomes as material for discussion or re-casting. The longer a work has been out, the more likely it is that other authors will have encountered it and wish to build upon it or incorporate it into their own subsequent works.

Copyright provides control over the production of derivative works based in part on copyrighted material. In certain circumstances, this control results in monopoly higher costs and lower production of new creative works. Many new creative works are built in part out of materials from existing works.[25] Improvements in the technology of search and recombination continue to expand the economic importance of new creation based upon old materials.

As Ronald Coase and many others have pointed out[26], economic efficiency is best promoted by legal arrangements that minimize transaction costs. Here, a limit on the duration of control rights over derivative works tends to reduce transaction costs, which give new creators less incentive to produce.[27]

Why will authors themselves, for-profit publishers, the recording industry or the motion picture industry give away their products when they can renew the protection? The free access to those works which would only produce further anecdotal incomes

---

24 *See* Liu, Joseph P., Copyright and Time: A Proposal. *Michigan Law Review, Vol. 101, No. 2,* (2002).

25 For example, new fiction re-tells old stories, new documentaries re-use historical footage, and new music re-mixes and transforms old songs.

26 *See* Coase, R., The Problem of Social Cost, 3 . *L. & Econ. 1* (1960).

27 *See* Alfaro, J., La infatigable extensión del derecho de autor: un poco de análisis de los costes y beneficios, *Blog Derecho* Mercantil, 15 Nov. 2011, available at http://derechomercantilespana.blogspot.com/2011/11/he-encontrado-el-escrito-de-alegaciones.html (13 Aug. 2013).

might stimulate sales of other future or even past and still-protected works from the same author. This can be easily seen with the key role that free digital giveaways are playing in the promotion of exhibitions, motion pictures, music or books, in which artists participate for free in certain activities in order to get their popularity increased and, indirectly, achieve eventual sales.[28] [29]

Copyright protection gives incentives for creation but at the same time monopoly rents cause both static and dynamic welfare loss to society. Copyright provides owners of the copyrighted material with the opportunity to earn returns. These returns must be generated at the expense of consumers. Copyright safeguards the incentive to create works generating creation fixed costs, at the expense of the potentially marginal costs of dissemination of works and creative re-use.[30]

2.4. Wife Says He Was Cleaning Weapon: Why Enlarging the Public Domain Is Not a Suicide

Copyright law already recognizes the necessity of disseminating the works freely, to some extent, through the limited copyright term. As their copyright terms expire, works pass from protected status into the public domain where they can be freely built upon, transformed, re-cast and re-imagined by others. The eventual passage of works into the public domain is an essential feature of our existing copyright structure.

All authors generally benefit from being able to build upon the ideas of others, and that they all share an obligation of some kind to prior authors. Thus, the eventual passage of an author's work into the public domain can be seen as part of the bargain that the author strikes in creating a work that inevitably builds upon the creative labor of those who have preceded him. To the extent that an author himself has built upon the creative labor of others before him, he has a moral obligation to similarly permit those coming after him to build upon his labor. The idea is that authors have a moral obligation to help replenish the public domain.

There seems little reason to fear that once works fall into the public domain, their value will be substantially reduced based on the amount or manner in which they are used. We do not claim that there are no costs to movement into the public domain, but,

---

28 *See* Lessig, L., *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, New York, The Penguin Press, 2004.

29 *See* Harfoush, R. 'JK Wedding Dance – The Evolution of Viral Marketing', http://www.rahafharfoush.com/2009/08/jk-wedding-dance-the-evolution-of-viral-marketing/.

30 *See* Hugenholtz, P. B. and Senftleben, Martin, Fair Use in Europe: In Search of Flexibilities (November 14, 2011).

on the opposite side of the ledger, there are considerable benefits to users of open access to public domain works. We suspect that these benefits dramatically outweigh the costs.

The academic literature tells two stories about what happens to works when they fall into the public domain. First, some economists suggest that an absence of copyright protection for intangible works may lead to inefficiencies because of impaired incentives to invest in maintaining and exploiting these works.[31] Why sell a work that others can also exploit for free and erode your market? Together with this under-exploitation hypothesis, others have argued instead, from a behavioral economics perspective, that when works fall into the public domain, they become attractive targets for exploitation because no license fee need be paid to the former owner of the work. Despite potential competition, exploitation will occur, just as it does in other markets where no one has a monopoly over the object of exploitation, e.g. the markets for string, milk or pencils. The data collected by platforms like Amazon demonstrates the power of the second hypothesis: that books and music become more attractive targets for exploitation after they fall into public domain.[32]

3. ALLOCATIONAL GOALS VS DISTRIBUTIONAL POINTS: TAKE THE MONEY AND RUN

Copyright itself is not an incentive mechanism, but it does allow an incentive mechanism, namely contracts, to operate. If the relationship between creator and investor –publisher/producer– with respect to duration, royalties and options can be negotiated as a bilateral legal relationship *sans droit d'auteur*, it is only by conceptualizing the further relationship of right holders to competitors and consumers that the regulatory function of copyright statutes become visible. In limiting competition, copyright statutes may enable right owners to charge higher prices. Empirically, it still remains an open question if this translates into higher earnings for the creator.

One of the most important arguments or rationales of copyright reflects notions of natural justice: authors' rights are not created by law but always existed in the legal consciousness of man.[33]This rationale presuppose that copyright vests in the author as creator of the work. This natural allocation principle is, indeed, reflected in the general

31 Landes, W. and Posner, R., Indefinitely Renewable Copyright, *70 U. CHI. L. REV.*, PP. 471-475. (2003).

32 *See* Heald, P., How Copyright Makes Books and Music Disappear (and How Secondary Liability Rules Help Resurrect Old Songs). *Illinois Program in Law, Behavior and Social Science Paper No. LBSS14-07*. (2013).

33 Ploman, E.W. and Clark Hamilton, L., *Copyright. Intellectual Property in the Information Age*. London, 1980, p. 13.

rule that copyright originates with the originator of the work. In fact, in most countries of the world, copyright is 'author's right' by definition, if not by name.

What is surprising then is that in practice nothing much of this allocation principle remains. Professional authors only rarely own the copyrights in the works they professionally produce. This is true not only for the millions of intellectual workers producing works under employment contracts, or otherwise 'for hire', but also for independent creators.

However, the intermediaries have never managed to deprive the authors from the one right that, more than anything else, represents the ethical core of the *droit d'auteur*: the moral right. The *droit moral* offered the authors at least a modicum of protection against abusive producer practices, such as unauthorized first publication, incorrect crediting or mutilation of the work. In some European countries, the moral right also provided the foundation for a number of further reaching author-protective provisions.[34]

It is one of the ironies of the Internet, that now 'publishing without publishers' is finally becoming a reality; authors are forced to assign their rights to publishers and other producers on an unprecedented scale. In the digital era, author's rights have become the authors' only by name. The producers have run away with the rights –so the money–, as in the early days of copyright. High timer to change the course of history once again, and return the rights where they belong: with the authors of works of literature, science and art.

Doesn't the existing repertoire of remedies under private law provide sufficient protection? Indeed, depending on the law applicable to the contract, several instruments available under general contract law may protect authors against unfair provisions in copyright contracts:

- the principle of 'fairness' or equity, that may supplement, or even an override, unfair contractual terms in certain jurisdictions;
- rules prohibiting unfair terms in standard agreements, or unconscionable contracts; and
- provisions allowing the revision or rescinding of a contract if unforeseen circumstances would make unaltered execution of the contract unjust.

However, even if authors might benefit from these rules in a given situation, general private law suffers from a fundamental flaw: its normative content is minimal. Contract law does not inform authors or intermediaries of the (un)reasonable nature of a specific contractual provision. Authors with a grievance may take a publisher to court after the fact, but in practice will be very hesitant to do so.

34 Both in Austria and Germany the moral rights inspired doctrine of monism –economic and moral rights are two sides of the same coin-led to the rule, still existing, that copyrights cannot be assigned or transferred.

Collective bargaining –on behalf of employed authors, or even 'organized' freelance creators– may restore the lack of balance in copyright contracting, and lead to a more equitable allocation of rights among authors and producers. However, in some countries, including United States and Germany, freelance authors are barred from collective bargaining for reasons of anti-trust law. Moreover, even absent such restrictions, freelance authors are often hesitant to organize themselves in guilds or unions. Many authors have elected to live the life of an independent creator not out of social or economic necessity, but as a matter of principle.

3.1. The proposal

Empirical data indicates that the investment horizon in cultural industries is well below 10 years.[35] There is also compelling evidence that the most intensive commercial exploitation takes place at the beginning and the end of the exclusive term.[36]However, setting a term that rationally balances under-production and under-use of copyright works is closed as a policy option, as international and European law stands. Still, the idea that works that are not being exploited should lose protection to the degree that they can be used by others is consistent with general principles of law. We find similar principles in the law of real property –landowner may lose title if rights are not asserted–, in competition law –compulsory licenses–, or contract law –revision and termination.

Compulsory registration of copyright works contravenes the Berne Convention, and altering that would be extremely cumbersome, but it does not prevent the development of a national voluntary scheme.[37] In fact, there are many 'private-national' registration systems, such as ISBN for books that already requires information from authors by publishers and copyright libraries. Right holders who have published works often register them with collecting society and collecting societies exist for all the valuable rights protected by copyright law. There are also private companies that have register works for the author in order to establish prior creation and provide evidence in the event of a dispute.

A registration system would enable the eventual introduction of a renewal system into the copyright term. Copyright could become more similar to a patent by having an

35 *See* Breyer, S., The Uneasy Case for Copyright: A study of copyright for books, photocopies, and computer programs, *Harvard Law Review*, vol. 84, no. 2, pp. 281-351. (1970/71).

36 *See* St. Clair, W., *The Reading Nation in the Romantic Period*, Cambridge University Press. (2004).

37 Now, unless you know for sure that something is in the public domain, you dare not use it, even if you can't locate the author in order to take a license. This has created a rights-clearance nightmare for any conscientious person who wants to builde upon pre-existing works or make them available.

initial term of protection of a work, say 10 years, renewable for further terms.[38] The advantage of this is twofold: it enables a 'use-it-or-lose-it' regime to function and, more relevant to the economics of copyright, it enables the market to function better in valuing a work. The vast majority of works are anyway out of print because they are deemed to have no commercial value while the copyright is still valid. Knowing that renewal would be necessary would also alter contractual terms between creators and intermediaries, thereby improving the efficiency of contracting and the prospect of fairer contracts.[39]

A more drastic version of this scenario has been proposed by Landes and Posner[40]: in keeping with trademarks, copyright would become perpetual with renewal required at stated intervals. But the incentive to renew only exists for protecting works that the right holder considered to be valuable. Unrenewed, so lacking value, works would go into the public domain, thereby overcoming the widely recognized problem of orphan works. Landes and Posner were already concerned with the considerable waste of resources employed in lobbying for extensions to copyright something that would be preempted by their scheme.

Other changes that could be considered relate to altering the focus of copyright more towards protecting the initial creator than subsequent right holders; this might be done by raising the requirement of originality, which has a very low threshold. With the development of social networking and other internet-based activities, the explosion of user-created copyright material has surely altered copyright law's intention of encouraging of learning, as well as leading to considerable unauthorized use of other's copyright material. Again, registration of works would reduce the problem of the excessive quantity of protected material and might deter unauthorized use too.

The regulation of collective rights administration could well be informed by more intelligent economic thinking than has so far been applied. That is a complex process that includes fragmentation of rights in a particular medium, such as music, art, literature, broadcasts, setting license fees for specific rights for their use in widely varying circumstances and developing formulae for distribution of revenues to individual right owners, including remunerations from levies and compulsory licenses and the like, registering lists of works provided by members or others who wish to license them collectively, maintaining a database of details of right owners and distributing monies to nationals and transfer credit to sister collective tights organizations abroad. Regulation and any moves to introduce competition needs to take all these activities into account.

38 This was the provision in the Statute of Anne, with 14 years renewable terms.

39 *See* Kretschmer, M. Copyright Term Reversion and the 'Use-It-Or-Lose-It' Principle. *International Journal of Music Business Research* (IJMBR) – ISSN 2227-5789 Issue 1, no. 1, April 2012.

40 Landes, W. and Posner, R., Indefinitely Renewable Copyright, *University of Chicago Law Review*, 70(2); pp. 471-518. (2002).

It seems that, finally, copyright does not always ensure a fair return for creators and performers. We should then revise the foundations for the ownership of rights, not the reward they gain. Copyright-'s rewards always come through the market, even where institutional arrangements have been put in place by the state to ensure that copyright is administered fairly. And so do its costs.

Our *de lege ferenda* proposal then is to legislate a simple rule that copyright should be registered for an initial term of 10 years, upon a fee, after which it will revert again to creator, in case he has transferred the rights. After those 10 years, the author would have the 'opt in-opt out' choice of:

- paying again the fee for another period of protection; or
- abandoning the work.

The challenge for the legislator will be to create a simple and transparent scheme which would reduce the frictional costs of licensing for both exploited and non-exploited works.

3.2. We Shall Overcome: Resurrecting Copyright Formalities

Constitutive and renewal formalities would play an important role in our model, as filtering instruments between works for which authors desire copyright protection and those for which they do not. If authors must fulfill a formality before their works are eligible for protection, they are obliged to make an initial assessment of whether or not their works sufficiently commercially valuable to warrant protection, i.e. whether the expected revenue of royalties would exceed the costs of completing the formality. The same assessment must be made if copyright is subject to a renewal formality. If the assessment appears favorable, authors are likely to fulfill the formality so as to secure protection for their works. If not, they most likely would refrain from doing so and the work will enter the public domain. Thus, in their capacity as filtering instruments, formalities may greatly enhance the free flow of information, in contrast to the present situation, in which each and every original work of authorship is automatically covered by copyright, constitutive and renewal formalities may substantially enlarge the number of works in the public domain[41].

Second, formalities may fulfill important signaling functions for the public. If, in a system where copyright protection relies on formalities, works for which no protection is desired are easily identifiable as being unprotected (e.g. if no notice is attached to the work or if the work has not been registered or deposited in a public registry), it is

41 *See* Van Gompel, S., Formalities in the digital era: an obstacle or opportunity?, *Global Copyright: Three Hundred Years Since the Statute of Anne, from 1709 to Cyberspace*, Cheltenham: Edward Elgar 2010, pp. 395-424.

instantly recognizable when a work resides in the public domain and thus can be used without prior authorization. This will significantly increase legal certainty for prospective users. More legal certainty will also be established if formalities provide indicators that facilitate the calculation of the duration of protection (e.g. if they would require authors and/or right owners to make relevant information concerning the author or date of first publication publicly available).

In the same vein, formalities may help to define and identify copyright-protectable subject matter. Constitutive formalities could provide the public with a clear indication of works for which authors claim protection. Obviously, this would not imply that these works automatically satisfy the substantive requirement(s) for protection. That will always be a matter for the courts to decide. Moreover, if copyright depended on registration, it is likely that registering bodies are given the discretionary power to refuse registering creations that obviously do not qualify as 'literary or artistic works' or lack sufficient originality (which should of course be subject to appeal by the applicant). This would help preventing all kinds of trivial works from entering the copyright arena. Likewise, it is possible that in cases of highly complex and technical works, applicants would be required to clearly indicate the elements of information for which they seek protection. Requirements of this kind are not uncommon in other fields of intellectual property law. In a patent specification, for example, the subject matter which the applicant regards as his invention must be particularly pointed out and distinctly claimed and, if necessary, be accompanied by a drawing.[42] Likewise, the registration of a design typically takes no legal effect unless the filing of a design sufficiently reveals its characteristics.

Even if only declarative of the right, formalities may grant a few key benefits. In general, they fulfill important evidentiary functions. The receipt of deposit or entrance in the registers, for instance, may establish prima facie proof of initial ownership of copyright.[43] Moreover, if the law requires a compulsory recordation of assignments or licenses, this may produce prima facie evidence of the legal transfer of ownership of copyright.[44] This enables authors and copyright owners to easily assert their rights and claim the title of property in a work. This may be particularly useful in conflicts where

42 §§ 112 and 113 of the US Patent Act (35 U.S.C. §§ 112 and 113). Likewise, art. 83 of the European patent convention requires a patent application to disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.

43 Under the nineteenth-century French legal deposit scheme, for instance, the receipt that was given upon deposit constituted prima facie proof of the property right on the work deposited. See art. 9 of the French Ordinance of 24 October 1814. Currently, voluntary registration schemes often provide for the same. See e.g. art. 53(2) of the Canadian Copyright Act (R.S., 1985, c. C-42): 'A certificate of registration of copyright is evidence that the copyright subsists and that the person registered is the owner of the copyright'.

44 See e.g. 17 U.S.C. § 205 under c and art. 53(2.1) and (2.2) of the Canadian Copyright Act.

the anteriority of authorship and/or the priority of a claim to the title must be resolved. In addition, even if the prima facie status of the claim allows the recorded facts to be rebutted by other proof, formalities may facilitate the exercise of rights by providing more certainty concerning the claim of copyright ownership.

Finally, formalities may constitute an indispensable source of information relevant to the clearance of rights. If authors and copyright owners were obliged to register their copyrights in a publicly accessible register and to duly record each assignment of rights, this would increase the availability of information identifying the work, its author(s) and current right owner(s) and other valuable information (e.g. about the date of first publication). To a greater or lesser degree, the same information would become available if authors were obliged to mark the copies of their works with a copyright notice. As a result, formalities may contribute noticeably to lowering transaction costs, to providing adequate legal certainty and to alleviating rights clearance problems, such as those of 'orphan works' (i.e. works the copyright owners of which cannot be identified or located). Hence, formalities may perform a key role in facilitating the licensing of copyright, thereby stimulating the legitimate use of copyright protected content.

4. CONCLUSION

It is apparent that creative industries interest groups regard copyright as a right that must be maintained or preferably strengthened rather than as a privileged granted for the wider benefit of society.

Copyright is essentially pragmatic and based on perceived net social benefit. However, focus by policy makers on the benefits of the creative industries in the form of their size and contribution to national economies emphasizes financial benefits and ignores cultural benefits as well as costs. Net social benefit is contingent on the state of technology and on cultural perceptions and therefore needs reviewing as technologies and consumptions habits change but so far this has just led to additions to statutes and extensions of copyrights duration and scope. Moreover, copyright is a line in the sand, and moving the line by changing the law redistributes costs and benefits between producers, intermediaries and consumers.

Resurrecting copyright formalities may be one of the most salient ways of dealing with the current needs. Because of their inherent capacities to enlarge the public domain, to define and facilitate the recognition of copyright-protectable subject matter, to improve the licensing of copyright protected works and to enhance legal certainty for users and copyright owners alike, formalities seem fit to address the challenges that copyright is presently facing.

At the end of the day, the success of copyright, and on author's rights which do not rely on economic justification, depends upon how well markets function for products

embodying creative works. That depends upon the good old laws of supply and demand. Copyright is an intervention in the market that should help not hinder them. Our initial choice for that help is to encourage registration and renewal of copyright rather than to forever strengthen copyright law.

Intellectual property, then, is not a response to allocative distortions resulting from scarcity, as real property law is. Rather, it is a conscious decision to create scarcity in a type of good in which it is ordinarily absent in order to artificially boost the economic returns to innovation… Economic theory offers no justification for awarding creators anything beyond what is necessary to recover their average fixed costs.

5. BIBLIOGRAPHY

Akerlof, G. et al. as Amici Curiae in Support of Petitioners, Eldred v. Ashcroft, 122 S. Ct. 1170 (2002). (no. 01-618), pp. 12-13

Handke, C., The Economic Effects of Copyright: The Empirical Evidence So Far, *Report to National Academies*, Washington DC, (2011).

Heald, P., How Copyright Makes Books and Music Disappear (and How Secondary Liability Rules Help Resurrect Old Songs). *Illinois Program in Law, Behavior and Social Science Paper No. LBSS14-07*. (2013).

Kretschmer, M. Copyright Term Reversion and the 'Use-It-Or-Lose-It' Principle. *International Journal of Music Business Research* (IJMBR) – ISSN 2227-5789 Issue 1, no. 1, April 2012

Landes, W. and Posner, R., Indefinitely Renewable Copyright, *University of Chicago Law Review*, 70(2); pp. 471-518. (2002).

Landes, W., and Posner, R., An Economic Analysis of Copyright Law, *18 J. Legal Stud.* 325, 333 (1989).

Lemley, Mark A., Property, Intellectual Property and Free Riding, *Texas Law Review*, Vol. 83, p. 1031, 2005.

WEBSITE BLOCKING: EVOLUTION OR REVOLUTION? 10 YEARS OF COPYRIGHT ENFORCEMENT BY PRIVATE THIRD PARTIES

Ellen Marja Wesselingh
The Hague University of Applied Sciences

ABSTRACT: Copyright enforcement by private third parties –does it work uniformly across the EU? Since the inception of Napster, home copying of digital files has taken a flight. The first providers of software or infrastructure for the illegal exchange of files were held contributory or vicariously liable for copyright infringement. In response, they quickly diluted the chain of liability to such an extent that neither the software producers, nor the service providers could be held liable. Moving further down the communication chain, the rights holders are now requiring Internet Service Providers (ISPs) that provide access to end customers to help them with the enforcement of their rights. This article discusses case-law regarding the enforcement of copyright by Internet Access Providers throughout Europe. At first glance, copyright enforcement has been harmonised by means of a number of directives, and article 8(3) of the Copyright Directive (2001/29/EC) regulates that EU Member States must ensure the position of rights holders with regard to injunctions against ISPs. Problem solved? Case law from Denmark, Ireland, Belgium, Norway, England, The Netherlands, Austria and the Court of Justice of the EU was studied. In addition, the legal practice in Germany was examined. The period of time covered by case law is from 2003 to 2013, the case law gives insight into the differences that still exist after the implementation of the directive.

KEYWORDS: Copyright, enforcement, case law, EU, intermediary service providers.

1. INTRODUCTION

In the past twenty years, the media landscape has changed drastically. The dissemination of creative works of any kind used to be controlled by professional parties. Consumers were consuming media, the re-use of existing media –for example playing songs in a theatre– was regulated with licenses and neighbouring rights. This has changed. Transaction and distribution costs have gone down due to the availability of digital media, making it possible for consumers to become producers and distributors of materials. These new opportunities for sharing have both good and bad effects. A positive effect can be found in some scientific communities where Open Access is slowly becoming the norm. A negative effect can be found in the peer-to-peer (P2P) file sharing facilitated by entities like The Pirate Bay. This new «norm» of sharing has created friction with the old system of copyright protection.

In the beginning of the twenty-first century, P2P file sharing was enabled in a more or less centralised way; most well-known is probably the Napster case (A&M Records v Napster, 2001). The company Napster was consequently held legally responsible for copyright infringement: by allowing users to infringe copyright directly, Napster committed contributory (§48-49) and vicarious copyright infringement (§60). Essential elements were that Napster provided the software for the user, maintained on its own servers search index software that enabled the connection and provided a hotlist of users of interest also currently logged on to the Napster server (§10-11). The court did not rule the mere existence of the Napster system as a ground for contributory and vicarious liability (§84-85).

The Napster case inspired other software developers to build different systems, with less centralised indexes. This decentralisation eventually led to the model used by The Pirate Bay. This website started in 2003 and has grown to one of the largest file sharing facilitators (website The Pirate Bay, 2014). The website started as a Bittorrent tracker; a list of so-called torrents that identify which file can be found where (Pouwelse, Garbacki, Epema & Sips 2005). The torrent files do not contain copyrighted materials themselves; they provide access information on where the material files can be found on the network. Rights holders successfully sued The Pirate Bay for (complicity in) copyright infringement in the EU Member States Sweden and The Netherlands (Sony Music Entertainment et al v Neij et al, 2009, B 13301-06) (Brein v The Pirate Bay, 2009, 428212-KG ZA 09-1092). As a result, The Pirate Bay switched to the provision of Magnet Links, files that do not point to an address on the network but to a cryptographic hash value that indicates the content of the file. This so-called Distributed Hash Table (DHT) technology was built to circumvent legal action by rights holders (Wolchok & Halderman, 2010, chapter 2).

By switching to this new technique, the operators of the P2P file sharing website no longer have any knowledge of the exact content of the files that the cryptographic hash value refers to, where companies like Napster and Grokster did have actual knowledge. Because the Internet has been mostly borderless in the past years, it has been very difficult for the nationally organised legal systems to enforce the shutdown of websites facilitating P2P file sharing. When being targeted with legal action, the operators simply move their business to another jurisdiction and the whole process of shutting down the business by court order starts from scratch in the new jurisdiction. As a result, the rights holders have moved down the chain of communication, away from the service suppliers of a specific P2P file sharing service towards the supplier serving the end customer Internet access. When we look at a model of communication, this process can be depicted as shown in figure 1.

The next sections discuss that process. This article uses the terminology Internet Service Provider (ISP), which encompasses all types of services, including providing end customers with Internet access, in which case the ISP will be named Internet Access Provider.

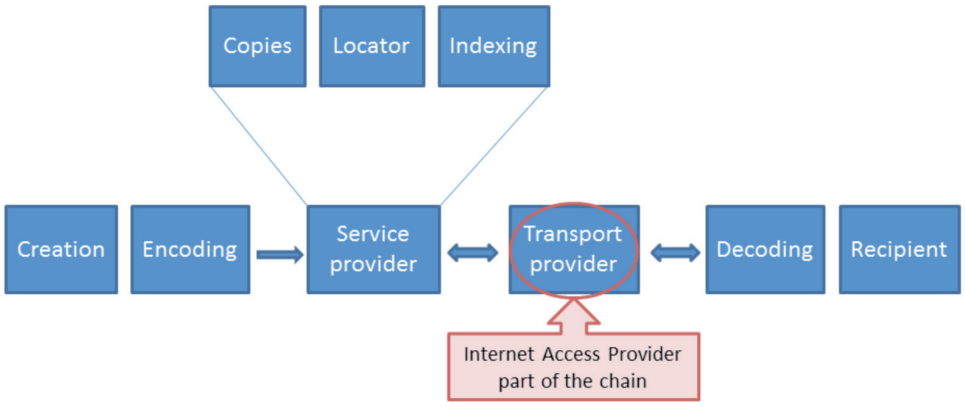


Figure 1: a model of transport of information. The model is based on the models of Shannon-Weaver Mathematical Model (1949) and Schramm's Model of Communication (1954) (see annex). Creation: the conceptualisation of a creative idea. Encoding: deciding in which format to publish the creative idea: print, sound, visual, et cetera. The "Service provider" is the provider of the platform that enables P2P exchange. The Internet Access Provider is one of the Transport providers (the provider enabling access to the recipient in this figure). It must be noted that noise can be added in any stage of the process.

2. HARMONISATION OF COPYRIGHT ENFORCEMENT IN THE EU

The original maxim was to enforce copyright (and related rights) at the source. Rights holders would sue the service provider (operator of the website containing the infringing materials or linking to infringing materials), such as in the Napster case.[1] Even Grokster, which had decentralised the business to avoid liability, was still held liable because it actively promoted copyright infringement by use of its service (Ricketson & Ginsburg, 2006). As discussed above, this model no longer works due to the ease with which service providers can move their business to another jurisdiction. The rights holders that wanted to enforce their copyrights had a few other options: either suing the end user, or forcing the end users' («mere conduit») internet access providers to block the infringing website. The latter is what most copyrights owners' representatives throughout the EU do.

At a first glance, in the European Union the enforcement of copyright has been harmonised in the Information Society Directive (2000/31/EC), the Copyright Directive (2001/29/EC) and the Copyright enforcement Directive (2004/48/EC). The Euro-

1 Many cases followed: Grokster/Kazaa, E-donkey, Limewire, FTD, Mininova, Newzbin, Kino to name just a few.

pean Union strives towards a single market and encourages the establishment of a level playing field in the telecommunications sector because that would form the foundation of said single market. The single market offers opportunities to legal business as well as illegal business, and the EU would like to encourage legal business while at the same time fight the infringement of rights of those doing legal business. Preamble section 59 and article 8 of the Copyright Directive are a reflection of the recognition that the services of intermediaries may be used for infringing rights of others in the digital world.

Section 59 of the preamble of Copyright Directive 2001/29/EC states: «*In the digital environment [..] services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries* [Internet Access Providers] *are best placed to bring such infringing activities to an end*. [..] *rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network*. [..] *The conditions and modalities relating to such injunctions should be left to the national law of the Member States*.» and article 8 states: «[..] *3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right*.» There is some harmonisation, but the exact implementation of the instrument of injunction is left to the Member States.

3. BLOCKING OF COPYRIGHT INFRINGING WEB SITES BY THIRD PARTIES

In Spain, rights holders have tried to bring to court individual end customers in an effort to stop copyright infringement. Rights holders' representative Promusicae sued ISP Telefónica for the personal details of customers behind IP addresses that were found to engage in P2P file sharing, in 2005. In January 2008 the European Court of Justice found that the directives regarding copyright do not require Member States to oblige the communication of personal data in civil proceedings, but that the Member States may implement such measures in accordance with Community law, such as the principle of proportionality (Promusicae v Telefónica). Similar proceedings happened in Ireland in 2005 ([2005] IEHC 233). However, turning to individual end customers has not become mainstream practice in Europe, the rights holders have mostly turned to ISPs to block the content rather than bringing individual citizens to court. In this section case law from various European countries regarding the blocking of P2P facilitating websites is discussed in a more or less chronological order.

3.1. Denmark: the early years

The first cases in Denmark were directed at Internet Access Providers to identify FTP (File Transfer Protocol) service providers serving copyright infringing materials

from their servers. In several court cases from 2003 to 2006 (TDC Totalløsninger v IFPI), the Internet Access Providers were ordered to provide the contact details of the FTP operators. From 2006 onward, P2P file sharing service providers were targeted by rights holders. Because these service providers operated abroad, the Danish Internet Access Providers were ordered to block the websites. The case of the rights holders (represented by IFPI Denmark) against Tele 2 A/S was decided in the first instance on 25 October 2006 (Aller International v Tele2). The court ordered Tele2 to block the website www.allofmp3.com, followed by a second decision in which Tele2 was ordered to block www.mp3sparks.com on 15 August 2007.

The case IFPI Denmark v DMT2 A/S was decided in the first instance on February 5th 2008 (Bailiff's Court of Frederiksberg). The court ordered the blocking of the website www.thepiratebay.org and its subpages and subdomains, without further specification of the technical measures to be implemented by the Internet Access Provider to comply with the order. The blocking order was appealed by the provider (High Court, 26 November 2008) and finally decided on May 27, 2010 by the Supreme Court (UfR 2010:2221-2230). In the first instance, no specific technical measures were considered; the court sufficed with a general order for the Internet Access Provider to take the necessary measures to prevent access. On appeal, four specific measures were considered: hardware or software content filtering (Deep Packet Inspection or DPI),[2] installing a proxy,[3] blocking DNS traffic,[4] and blocking IP addresses.[5] The same court already considered these four measures in an appeal case of 2 August 2006.[6]

Of these four options, the Supreme Court only considered DNS blocking a viable option. DPI is considered to be too expensive for Internet Access Providers, both economically and in data traffic delay. The proxy solution is troublesome with encrypted (HTTPS) traffic, which is frequently used in Virtual Private Networks (VPNs). IP-addresses often change frequently and may host more websites than just the infringing site, and apart from these issues IP addresses were considered to be personal data in the earlier judgements regarding FTP-server operators. The drawback of DNS blocking, that it can be easily circumvented, is not considered to be a problem, the courts are of the opinion that «*Blocking at the DNS-level are generally sufficiently effective*» (Sonofon v IFPI Danmark). The Internet Access Providers claimed «*the prohibition and injunction is*

2 UfR 2010:2224. «Metode 1: Installation af hardware og software mellem ISP'ens internetforbindelse og deres kunders adgang.» The specific technology mentioned is Content Filtering by Sonicwall.

3 UfR 2010:2224. «Metode 2:Etablering af en såkald Proxy.»

4 UfR 2010:2225.

5 UfR 2010:2225.

6 UfR 2010:2229.

not sufficiently clear and precise, not proportional and subsidiary»[7] but the Supreme Court disagreed and upheld the order to block The Pirate Bay website with the use of DNS-blocking.[8]

Preventing access to websites by Internet Access Providers using DNS-blocking is considered a solution in Denmark. In January 2013, six websites were blocked by all Internet Access Providers in Denmark for enabling the illegal exchange of copyrighted materials. The list is growing; in October 2013 a total of 10 websites were listed.[9]

3.2. Belgium: the first references to the CJEU

In Belgium, blocking of websites by Internet Access Providers was also the subject of discussion in court cases. The Belgian court of first instance discussed in detail what type of technology the Internet Access Provider may use to implement the blocking order: a network appliance using Deep Packet Inspection (Hughes, Mady & Bourrouilhou 2007). However, the blocking order by the court was of a more general nature, stating that the Internet Access Provider shall stop copyright infringements by disabling file sharing through P2P, without giving technical specifications.

The Belgian appeal court found reasons to ask prejudicial questions regarding the issuance of a blanket order upon an Internet Access Provider to install a filtering system for all its' customers to the Court of Justice of the EU in Luxembourg (Scarlet v Sabam). In answering the prejudicial questions, the Court of Justice of the EU found that no Deep Packet Inspection shall be ordered in this type of case. The Court defined the steps that a DPI system performs (Scarlet v Sabam, 24 November 2011):

1. To identify within all of the electronic communications the peer-to-peer traffic;
2. Identify with the peer-to-peer traffic files containing works that may be subject to a copyright claim;
3. Determine which files are actually being shared unlawfully;
4. Preventing the availability of these files that contain works subject to a copyright claim.

The Sabam v Netlog case (16 February 2012) concerned a social network instead of an Internet Access Provider. However, the Court concluded similar: no service pro-

7 UfR 2010:2229.

8 UfR 2010:2230.

9 Tele Industrien provides a list (http://www.teleindu.dk/brancheholdninger/blokeringer-pa-net-tet/), in January 2013 the following websites were listed: www.allofmp3.com (2006/7), www.mp3sparks.com (2006/7), www.thepiratebay.org (2008), www.thepiratebay.se (2012), www.homelifespain.com (2012), and www.grooveshark.com (2012). www.dreamfilm.se, www.swefilmer.com, www.primewire.ag and www.movie4k.to were added in October 2013.

vider can be required to implement a general monitoring obligation that is unlimited in time, monitors all users without prejudice for an unlimited period of time and must be funded exclusively at the cost of the service provider. This is in line with previous case law concerning a service provider enabling the online trade of physical goods (L'Oréal v Ebay). In this case service providers may be required to block activities involving trademark infringement (including future infringements), but there can be no general monitoring obligation. According to the Court, the prohibition of a general filtering obligation under preamble sub 47 and article 15(1) of the Information Society Directive (2000/31/EC) is applicable to Internet Access Providers (Scarlet v Sabam) as well as Social Networks as hosting providers (Sabam v Netlog).

In both the Scarlet v Sabam and Sabam v Netlog cases the Court considered the human rights as defined in the Charter of Fundamental Rights of the EU, most notably the freedom to do business (Scarlet §46, Netlog §44), privacy of individual customers (Scarlet §51, Netlog §48-49) and freedom of expression (Scarlet §52, Netlog §50). The material questions on whether one right or the other must prevail in a specific case must be left to the national court, especially since statutory exceptions to copyright exist among EU Member States (Scarlet §52, Netlog §50).

3.3. The United Kingdom: a shift in technologies prescribed

In the UK, a number of cases went all the way to the High Court. After unsuccessfully ordering the website Newzbin to close down in 2010, the court ordered Internet Access Provider British Telecom (BT) to block the website Newzbin2 in July 2011 (Fox v BT, [2011] EWHC 1981). In April 2012, providers Sky, BT, Everything Everywhere, TalkTalk, Virgin Media and Telefónica were ordered to block The Pirate Bay (Dramatico v B Sky B, [2012] EWHC 268). In February 2013, the same providers were ordered to block the websites KAT (Kickass Torrents), H33T and Fenopy (EMI v B Sky B, [2013] EWHC 379). Without being exhaustive, the list shows that blocking is a popular method.

Based on section 97A CDPA 1988, which implements article 8(3) of the Copyright Directive,[10] the rights holders wanted that «*The Defendant* [access provider British Telecom] *shall prevent its services being used by users and operators of the website known as NEWZBIN and NEWZBIN2 to infringe copyright.*»[11] Regarding the technology to be implemented, the revised request was that «*The Respondent* [British Telecom] *shall adopt the following technology directed to the website known as Newzbin or Newzbin2 currently accessible at www.newzbin.com and its domains and sub domains. The technology to be adopted is:*

10 Fox v BT §153 & §158.

11 Fox v BT §11.

(i) *IP address blocking in respect of each and every IP address from which the said website operates or is available* [..].

(ii) *DPI based blocking utilizing at least summary analysis in respect of each and every URL available at the said website and its domains and sub domains* […].»[12]

We see that the High Court orders Deep Packet Inspection, and specifies in detail that all web addresses (Uniform Resource Locators or URLs) of all websites that are being visited by all the BT customers must be checked, in order to find the main domains and the subdomains operated by Newzbin, and subsequently filter out these domains. In the final order given, it was reiterated what type of technology the Internet Access Provider shall use to implement the blocking order.[13] The reasoning in the Newzbin case shows that the Court did consider the issues of and freedom of expression (§76-77, 164) and the right to property (§78). Privacy was not explicitly considered, reference was made to the Privacy directive 95/46/EC (§79 and 88) and to case law of the European Court of Justice (§155). The issue of freedom of doing business was not considered by the Court in its weighing of rights.

Nearly a month after the Newzbin case, the Court of Justice of the EU delivered its interpretation of the EU law in the Scarlet v Sabam case on 24 November 2011. This judgement clearly prohibited courts under EU law to order blocking of websites with the use of DPI techniques. From then on, the High Court issued blocking orders by application of different techniques:

«[…] The technology to be adopted is:

(i) IP blocking in respect of each and every IP address from which the said website operates and which is:

(a) notified in writing to the Respondent by the Applicants or their agents; and

(b) in respect of which the Applicants or their agents notify the Respondent that the server with the notified IP address blocking does not also host a site that is not part of the Newzbin2 website.

(ii) IP address re-routing in respect of all IP addresses that provides access to each and every URL available from the said website and its domains and sub-domains and which URL is notified in writing to the Respondent by the Applicants or their agents; and

(iii) URL blocking in respect of each and every URL available from the said website and its domains and sub-domains and which is notified in writing to the Respondent by the Applicants or their agents.» (Dramatico v Sky, 2012).

12 Fox v BT §12.

13 Fox v BT Order, issued 26 October 2011.

At the time of this writing, many websites in the United Kingdom are blocked (well-known examples are www.newzbin.com and www.thepiratebay.org), but due to the various methods used by ISPs it remains uncertain how many websites exactly are blocked. However, the list contains at least 150 named websites that are being blocked according to an activist collection page (Immunicity, 2014).

3.4. Austria: not too specific, are generic blocking orders the answer?

In Austria, article 8(3) of the Copyright Directive is implemented in §81 of the federal law regarding the copyright on works of literature and art and concerning neighbouring rights.[14] Court judgements are phrased in two stages: first, a blocking order is given to an Internet Access Provider, ordering the provider to take whatever measures are necessary to block a website without specifying in detail when and technically how the website(s) shall be blocked by the access provider. This issue creates legal uncertainty («*Rechtsunsicherheit*») of subjects regarding the application of the law in a certain case: an Internet Access Provider is not really capable to judge the validity of a blocking request by a private party, especially regarding the requirements of «systematic» and «regular» infringement as argued in court cases. The technical measures taken by the provider must be tested by an independent judge upon request of rights holders. A ban («*Erfolgsverbot*») and independent judgement are not necessary mutually exclusive in the opinion of the Austrian government (Wesselingh, 2013).

The Austrian High Court asked prejudicial questions about the procedure to the European Court of Justice (UPC Telekabel Wien, 2012, C-314/12). The questions referred to by the Austrian High Court ask whether the website illegally providing copyright protected material is using Internet Access Provider services when customers of that access provider download copyrighted content, and if downloading for private use from an illegal source is permitted if providers of illegal material are not using the services of the access providers mentioned in the first question. The third prejudicial question asked whether a blocking order without specific technical implementation is considered compatible with EU Law, the final question concerned whether the cost of implementation would be a prohibiting factor for a blocking order.

In November 2013, the Advocate General issued his opinion on these questions, the judgement of the Court followed on 27 March 2014. A website illegally providing copyright protected material is using the services of an Internet Access Provider whose customers access that copyright protected material (Advocate General §59, Court §40). According to the Advocate General, a so-called «*Erfolgsverbot*» (a generically formulated blocking order for a specific website) that is being ordered upon a third party that does

14 Bundesgesetz über das Urheberrecht an Werken der Literatur und Kunst und über verwandte Schutzrechte.

not have a contractual relationship with the infringer, is contrary to the requirements as set in article 8(3) of Copyright Directive 2001/29 (§71), not providing a fair balance between enforcement of copyright and freedom of expression (§82) and freedom of enterprise (§83). The Court did not find that EU law precludes this *Erfolgsverbot*, provided it does not hinder lawful information access and the measure is effective in preventing unlawful access(§64).

There are some potential issues with a generically formulated order without specification of the technical measures to be implemented by a third party to stop copyright infringement, notably the legal insecurity. However, given the fact that case law of the CJEU shows unequivocally that very specific and targeted solutions such as Deep Packet Inspection are not allowed, and there is a right to freedom of enterprise, a more generic blocking order which allows the third party to make choices of implementation seems an appropriate solution.

3.5. Norway and The Netherlands: no, yes, err... no (or maybe yes)

In most countries discussed before, the reasoning and exact implementation of the solution to copyright infringement via P2P networks is not similar in detail, but the outcome at the highest level of abstraction is similar: a website shall be blocked by the Internet Access Provider. In some countries the order is accompanied by detailed technical implementation requirements whereas in other countries the implementation is left to the access provider. However, there are even some exceptions to the blocking orders issued.

In 2010, the Norwegian Court of Appeals refused an interim measure in the application for a preliminary injunction by various rights holders. The rights holders had sought an order requiring an Internet Access Provider to cease contributing to infringements committed through the P2P exchange site The Pirate Bay. The Court of Appeals confirmed the rejection by the Court of first instance and refused the requested measure, since article 8(3) of the Copyright Directive was not specifically implemented in Norwegian law (Nordic Records v Telenor, 2010).[15] The Court noted that despite the fact that the dispute had been going on for several years, the rights holders had not started substantive proceedings to order Telenor to block The Pirate Bay (p. 22), indicating that the Appeals Court did not find an urgent reason for an interim measure.

In one Dutch case in summary proceedings, the court dismissed a blocking order sought in 2010 (Brein v UPC, 2010). The request for a blocking order was rejected based on proportionality (a minority of customers is infringing but the order concerns all customers), no concrete individualised infringement, not clear why it would not

15 Although Norway is not a party in the EU treaties, in practice it does follow EU law.

be possible to call to justice one or more individuals, and no individual users could be heard in court. Subsequent substantive proceedings before the court in The Hague in first instance, led to blocking orders imposed on all major Internet Access providers in 2012 (Brein v Ziggo, 2012) (Brein v UPC, 2012).

In appeal, the Court of Appeals in The Hague ruled in January 2014. The providers Ziggo and Xs4all had appealed the order imposed on them to block the websites of The Pirate Bay (TPB) in January 2012. The Court of Appeals reversed the order given by the Court of First Instance, reasoning that blocking is not effective when the total behaviour of Ziggo customers is taken into account (§5.12). The court introduced a new concept of effectiveness that includes use of other entry points to access illegally offered copyrighted materials, such as the availability of proxy services to go to TPB and also the use of different providers of copyrighted materials (§5.13). From the viewpoint of the administrators of TPB, they are less effective in their infringements due to the blockade (§5.12), but from a more general viewpoint the blockade is not effective. The court is not convinced about the argument that TPB is a test case, since it would have been quite easy for the complaining party (Brein) to add other big torrent providing sites to the affadit (kickass.to, torrentz.eu, Isohunt), as these parties do not have to be involved in the proceedings (TPB was not involved in this case either).

Dutch rights holders' representatives have announced to go to the High Court in a bid for cassation of the judgement to repeal the blocking order. Up until now, they seem wary to start civil procedures against large scale infringing individuals, or stop their efforts to bring large-scale file sharing to a halt.

4. DISCUSSION AND CONCLUSIONS

Where is all this fighting taking us? The EU has issued three directives that aim to provide effective protection of copyright, but the *de facto* situation is that many providers of platforms where copyrighted material can be illegally exchanged are situated outside of EU borders. This means these providers cannot be legally challenged in the EU, as the EU has no jurisdiction. In order to get an effective remedy, the rights holders turned to intermediary service providers, the Internet Access Providers whose customers access the material through the platform located outside the EU.

The Internet Access Providers mostly refuse to cooperate, leading to many court cases in which the rights holders seek orders to block specific websites. In many cases, the court actually grants a blocking order. However, there is a great deal of variety in the way providers have to comply with the order. In Austria, it is thought that the provider is best suited to consider and implement a specific measure. The order is only generically formulated, a practice that introduces legal uncertainty according to these providers (and the Advocate General at the CJEU). In the United Kingdom, providers have been

ordered in great detail how to implement the blocking order. Other EU countries have seen blocking orders with a level of detail in between these two extremes.

Occasionally, no blocking order was granted. In the latest case in The Netherlands, the Appeal Court reversed a previously ordered blockade. The representative of the rights holders (Foundation Brein), has announced it will appeal that decision. Meanwhile the discussion whether blocking websites by Internet Access Providers is effective or not continues. Both sides in the dispute have come up with research showing that their position is correct, while these positions are mutually exclusive: either a blockade is effective or it is not. One further step into the analysis of positions was done by the Dutch Court of Appeal, in that it separated the effectiveness from the viewpoint of the website and the viewpoint of the end user. Whether that provides the answer to the apparent contradiction remains to be seen.

At the moment, EU Member States have a margin of appreciation when implementing the EU Directives 2000/31/EC, 2001/29/EC and 2004/48/EC. The margin leads to differences in case law observed throughout the EU. In light of the ambition that the telecommunications market should be a single market throughout Europe, this seems an anomaly.

Until now, the rights holders' representatives in some EU Member States have shied away from going after the individual. With the rights holders having few other options left, they may in the future choose to start civil procedures against large-scale uploaders. In Germany, a legal practice has emerged in which certain legal firms target thousands of individuals each year. People downloading movies or watching streaming video received letters claiming copyright infringement and a transaction proposal involving hundreds of euros and the signing of a contract to not do it again, ever. Breach of that contract may cost thousands of euros. German government recently adopted a law to maximise the penalty sought, to mitigate the problem (Dedden, 2013).

The judgements of the CJEU are problematic from a copyright enforcement perspective as DPI is the only method currently available to distinguish legal P2P traffic from copyright infringing P2P traffic. Legal use of P2P traffic examples include synchronisation of servers (as Facebook does on its back-office network) and the sharing of Open Source software (such as operating system Linux distributions). Also, the various exceptions in the copyright laws provide for legal transmission of (parts of) copyrighted materials.

The current methods that are imposed by the courts are IP address blocking and DNS blocking. Both are rather crude instruments, indiscriminately blocking legal content and copyright infringing content based on the source. DNS-blocking of websites does not function as a very high threshold since there are sufficient methods available to bypass the blockade (Dilmpieri, King & Dennis, 2011) (Wesselingh, Cristina & Tweeboom, 2013) (Poort, Leenheer, van der Ham & Dumitruc, 2013). IP address blocking appears to do the job, but may only be imposed in cases where an infringing website is the only website behind an IP address. No case law on this subject matter is available today, although the

Yildirim case that was argued before the European Court of Human Rights provides some insight into what direction such case law might go (Yildirim v Turkey, 2012).

Case law is rapidly emerging at the highest level, with several cases before the Court of Justice. So far, the court has interpreted EU Law as prohibiting invasive techniques like Deep Packet Inspection for copyright enforcement. Recently the Court decided that EU Law does not prohibit any blanket type of injunction on third party service providers, with the provisions that lawful information must remain accessible and the measures taken must reasonably effective. These developments will probably lead to the techniques of DNS blocking and IP address blocking being the only tools that may be applied in the future, tools of which the effectiveness is under discussion.

5. BIBLIOGRAPHY

Directives

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ 2000 L 178, p. 1)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10)

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigenda OJ 2004 L 195, p. 16, and OJ 2007 L 204, p. 27)

European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, OJ L C 364/01, available at: http://www.refworld.org/docid/3ae6b3b70.html [accessed 7 March 2014]

Case law

- A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), affirming, 114 F.Supp.2d 896 (N.D. Cal. 2000)
- Stockholm District Court, 17-04-2009, Sony Music Entertainment et al v Neij et al, verdict B 13301-06, unofficial translation by IFPI, www.ifpi.org/content/library/pirate-bay-verdict-english-translation.pdf [accessed 28 February 2014]
- Rechtbank Amsterdam (Summary proceedings), 30-07-2009, Brein v The Pirate Bay, case 428212-KG ZA 09-1092, http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2009:BJ4298 [accessed 28 February 2014]

- Hof van Beroep (Court of Appeal) of Antwerp, 26 September 2011, Case 2010/AR/2541 VZW Belgian Anti-Piracy Federation v NV Telenet, m.nt. Van Eecke & Fierens, Larcier RABG 2011/18 pp. 1269-1287
- European Court of Justice, Productores de Música de España (Promusicae) v Telefónica de España SAU 29 January 2008 (Case C-275/06)
- High Court of Ireland, 8 July 2005, [2005] IEHC 233, EMI Records Ireland Ltd v. Eircom PLC, http://www.bailii.org/ie/cases/IEHC/2005/H233.html [accessed 18 December 2013]
- TDC Totalløsninger A/S v. IFPI Danmark asagent for Arcade Music Company et al., UfR 2006.1474 H (Supreme Court of Denmark, 10 February 2006 – Docket no. 49/2005)
- IFPI Denmark as agent for Aller International A/S et al. v. Tele2 A/S (Bailiff's Court of Copenhagen, 25 October 2006-Docket no. F1-15124/2006)
- IFPI Denmark v. DMT2 A/S-Fredriksberg Fogedrets Kendelse, 5 February 2008-FS 14324/2007, unofficial translation by Henrik Spang-Hanssen, Danish Supreme Court attorney-at-law, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1093246 [accessed 27 November 2013]
- Sonofon A/S (tidligere DMT2 A/S) v. IFPI Danmark-Østre Landrets 11. Afdelings kendelse af 26 november 2008 – Kæresag B-530-08, unofficial translation by Henrik Spang-Hanssen, Danish Supreme Court attorney-at-law, http://ssrn.com/abstract=1649682 [accessed 27 November 2013]
- Telenor (tidligere DMT2 A/S og Sonofon A/S) mod IFPI Danmark, Højesterets Kendelse (Supreme Court), afsagt torsdag den 27. maj 2010, Sag 153/2009, UfR 2010:2221-2230
- Hughes, J., and Mady, F. and Bourrouilhou, J., Translation Series: Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, Working paper http://ssrn.com/abstract=1027954 [accessed 24 October 2013], Tiscali later became Scarlet
- Court of Justice of the European Union (CJEU), Reference for a preliminary ruling from the Cour d'appel de Bruxelles (Belgium) lodged on 5 February 2010-Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM), Case C-70/10
- Court of Justice of the European Union (CJEU), 24 November 2011, C-70/10, Scarlet Extended NV v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) (Scarlet-Sabam)
- Court of Justice of the European Union (CJEU), 16 February 2012, C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (Sabam-Netlog)

- Court of Justice of the European Union (CJEU), 12 July 2011, C 324/09, L'Oréal SA et al v eBay International AG et al (L'Oréal-eBay)
- England and Wales High Court (Chancery Division), 28 July 2011, [2011] EWHC 1981 (Ch), Case No: HC10C04385, Twentieth Century Fox Film Corporation et al v British Telecommunications Plc, http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html [accessed 3 March 2014]
- England and Wales High Court (Chancery Division), 27 April 2012, [2012] EWHC 268 (Ch), Case No: HC11C04518, Dramatico Entertainment Ltd et al v British Sky Broadcasting Ltd et al, http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html [accessed 3 March 2014]
- England and Wales High Court (Chancery Division), 28 February 2013, [2013] EWHC 379 (Ch), Case Nos: HC12F4957, HC12F4958, HC12F4959, EMI Records Ltd et al v British Sky Broadcasting Ltd et al, available @ http://www.bailii.org/ew/cases/EWHC/Ch/2013/379.html [accessed 3 March 2014]
- Court of Justice of the European Union (CJEU), Reference for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 29 June 2012-UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Munich (Germany), Wega Filmproduktionsgesellschaft mbH (Case C-314/12)
- Hearing 20 June 2013, Conclusion of Advocate-General P. Cruz Villalón 26 November 2013, Judgement of the Fourth Chamber 27 March 2014 (Telekabel Wien), http://curia.europa.eu/juris/liste.jsf?language=nl&num=C-314/12 [last accessed 8 May 2014]
- Borgating Court of Appeals (Borgating Lagmannsretts), Nordic Records Norway et al v Telenor ASA (unofficial translation), 9 Feb 2010,
- http://hssph.net/NordicRecords_Telenor_NorwegianCourtofAppeals9Feb2010.pdf [accessed 20 December 2013]
- Court of First Instance The Hague (summary proceedings), 19 July 2010, Stichting Brein v Ziggo and Xs4all, http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2010:BN1445 [accessed 3 March 2014]
- Court of First Instance The Hague (Rechtbank 's-Gravenhage), 11 January 2012, case no: 374634/HA ZA 10-3184, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v ZIGGO B.V. and XS4ALL Internet B.V.,
- http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2012:BV0549 [accessed 3 March 2014]
- Court of First Instance The Hague (summary proceedings), 10 May 2012, case no: 413085/KG ZA 12-156, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v UPC Nederland B.V., KPN B.V., T-MOBILE Netherlands B.V., TELE2 Nederland B.V. and TELE2 Internetdiensten B.V., http://uitspraken.

rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2012:BW5387 [accessed 3 March 2014]

- European Court of Human Rights (ECtHR) second chamber, 18 December 2012, Ahmet Yildirim v. Turkey, request no. 3111/10

Articles and other sources

Website of The Pirate Bay: https://thepiratebay.se/about [accessed 21 February 2014]

Pouwelse J., Garbacki P., Epema D., and Sips H. (2005), *The Bittorrent P2P File-Sharing System: Measurements and Analysis*, in: Castro M. and van Renesse R. (Eds.): IPTPS 2005, Lecture Notes in Computer Science Volume 3640, 2005, pp 205-216

Wolchok S. and Halderman, J. A. (2010), *Crawling BitTorrent DHTs for Fun and Profit*, Proc. of WOOT (Washington, DC, USA, 2010)

Ricketson, S. and Ginsburg, J.C. (2006), *Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's KaZaa Ruling*, Columbia Public Law & Legal Theory Working Papers, Paper 0698. Retrieved February 27th, from http://lsr.nellco.org/columbia_pllt/0698

Website of blocked websites UK: https://immunicity.org/blockedsites [accessed 27 February 2014]

Wesselingh E.M. (2013), Notes from the oral hearing before the Court of Justice of the European Union (CJEU) on 20 June 2013

Dedden M. (2013), *Gesetz gegen unseriöse Geschäftspraktiken – was ändert sich im Urheberrecht?,* 27 June 2013, http://www.mucportal.de/2013/07/01/gesetz-gegen-unseriose-geschaftspraktiken-was-andert-sich-im-urheberrecht/ [accessed 3 March 2014]

Dilmperi A., King T., Dennis C. (2011), *Pirates of the web: The curse of illegal downloading. Journal of Retailing and Consumer Services*, 18 (2) 132-140

Wesselingh, E.M., Cristina, A.S., Tweeboom, N.M.G. (2013), *To Block or Not to Block?*, Working Paper, 4 June 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273453 [accessed 2 September 2013]

Poort J., Leenheer J., van der Ham J., Dumitruc C. (2013), *Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay*, Working paper, 22 August 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314297 [accessed 2 September 2013]

4

TERRITORIAL LIMITATIONS IN COLLECTIVE MANAGEMENT OF COPYRIGHT AFTER CISAC JUDGEMENTS

Anna Moscibroda
Research Group on Law Science Technology & Society
Vrije Universiteit Brussel, Researcher

ABSTRACT: In April 2013, the General Court of European Union granted the long-awaited series of judgements related to the collective management of performing rights in musical works. These judgements, concluding the number of appeals by collecting societies against the 2008 antitrust decision of the European Commission in the so-called CISAC case, resulted in partial annulment of said decision. In the CISAC decision, the Commission prohibited, inter alia, the concerted practice of territorial (national) licensing when technology allows for multi-territorial exploitation amongst the collecting societies. In all but one judgement, the Court annulled the decision as regards the concerted practice on the ground that its existence was not proven to the required legal standard. While those judgements do not allow for definitive conclusions as to the legality of territorial limitations in copyright licensing or the functions of collecting societies, in one disjoint judgement (relating to the appeal by Swedish society STIM which did not raise objections as to the sufficient proof of concerted practice) the Court upheld the Commission's assessment of the anticompetitive character of the territorial licensing limitations and arguably indicated its overall strict review of the justifications for the territorial monopolies in copyright licensing.

KEYWORDS: Collective Rights Management, licensing, copyright, competition law, CISAC.

1. INTRODUCTION

On 12 April 2013, the General Court of European Union ('the Court') delivered a number of judgements in an appeal against the so-called CISAC decision of the European Commission. The said judgements and the decision concern the operation of a number of collecting societies based in the European Economic Area (EEA) and managing authors' performing rights, and in particular the cooperation between these societies based on the reciprocal representation agreements. All societies concerned are members of the Confédération Internationale des Sociétés d´Auteurs et Compositeurs (CISAC), an umbrella association of national collecting societies around the world, facilitating the international cooperation between its members societies by, inter alia, promoting the model of the representation agreement which societies adopt in their bilateral relations. Certain clauses of that reciprocal agreement (namely membership and exclusivity clauses) have been subject to the Commission's antitrust intervention

and, subsequently, were prohibited in its 2008 CISAC decision.[1] So was a the concerted practice of limitation of licensing mandates to the single national territory by the societies concerned, despite the fact that certain forms of copyright exploitation (e.g. via cable retransmission, satellite broadcast or online) are multi-territorial in their nature. The Commission's decision opened a discussion on the compatibility of the traditional territorial model of collective management of copyrights with the EU competition law and internal market objectives, and –more broadly– on the functions of collective management of copyrights in the digital era and its desirable model.

The CISAC prohibition decision was appealed by nearly all collecting societies and by CISAC itself.[2] The Court's review of the CISAC decision resulted in its partial annulment: the Court sustained the Commission's finding as to the infringing character of the membership and exclusivity clauses, but it considered that the existence of the concerted practice was not proven to a sufficient legal standard, and hence annulled the decision on the related point. In one of the judgements, however, concerning the Swedish collecting society STIM, the Court accepted that the existence of the concerted practice and considered its anticompetitive character. This is also the only judgement that casts some light upon the Court's assessment of the anticompetitive character of territorial (national) mandates.

This paper summarizes and analyses all CISAC judgements together, and against their broader context (i.e. previous judgements and decisions regarding the collective rights management, and recent regulatory developments in the field) with an aim of assessing their implications and drawing common conclusions.

2. COLLECTIVE MANAGEMENT OF COPYRIGHT

2.1. Collective management: general remarks

Collecting societies have been established by authors themselves as early as in the 19th century,[3] in a reply to their practical needs. They were unable to individually manage and enforce their rights. Mass exploitation of music, facilitated by the technological development (e.g. broadcasting), made the individual management of rights of music

1 Case COMP/C2/38.698 – CISAC, Commission decision of 16 July 2008, further referred to as 'CISAC decision'.

2 A number of separate appeals have been submitted to the Court against (single) CISAC decision, leading to a number of separate proceeding and judgments (see infra, *note* 32).

3 Frabboni, M., M. (2009). Collective management of copyright and related rights: achievements and problems of institutional efforts towards harmonisation. In: Derclaye, E. le (ed.), *Research handbook on the future of the copyright*, Edward Elgar Publishing.

authors even less feasible: neither they had the capacity to control and license all acts of exploitation of their rights, nor they had the bargaining power to negotiate the licensing conditions, e.g. with broadcasters.[4] Therefore, the authors (or other right holders) authorize a collecting society to administer their rights, i.e. to license them, collect the fees and distribute them back to the right holders, monitor the use of works and enforce rights, if needed.

Traditionally, the activity of the collecting society covered one national territory. The authors joined the society operating in their own country, providing it with their rights (a repertoire). Hence, each society was able to manage only domestic repertoires. National societies collaborated with foreign societies by means of reciprocal representation agreements. A reciprocal representation agreement is an agreement between two collecting societies of two different countries when one society authorizes the other to license the exploitation of its repertoire[5] in the other society's territory. Thanks to reciprocal representation agreements, each collecting society is entitled to license not only its own domestic repertoire, but also the repertoire of all associated collecting societies. And thanks to the network of the reciprocal representation agreements each society was able to offer rights in the comprehensive (i.e. covering all world) repertoire of works (a «global repertoire»),[6] though only within their domestic territory.

Reciprocal representation agreements are the main instrument of cooperation between societies, and the main instrument for the licensing and enforcement of authors' rights abroad. However, their strictly domestic model of operation came under criticism as it did not suite certain forms of exploitation, e.g. satellite broadcast, internet broadcast or other types of online use which are multi-territorial in nature. The multi-territorial music users were forced to seek authorisation separately for each national territory involved, which arguably increased their contracting costs[7] and lead them to question the legitimacy of territorial monopolies of the collecting societies under the internal market and competition law.

2.2. Collective management: the EU legal framework

The economic aspects of copyright have been to large extent harmonised within the European Union. The key rights involved in the licensing of music are the reproduction

4 Uchtenhagen, U., (2011). Copyright Collective Management in Music. Geneva: WIPO, p. 11 and following.

5 Case 395/87 *Ministère Public v. Jean-Louis Tournier* [1989] ECR 2521, paragraph 17.

6 CISAC decision (see supra, *note* 1), paragraph 14.

7 KEA European Affairs, (2012). *Licensing music works and transaction costs in Europe*, KEA, http://www.keanet.eu/docs/music%20licensing%20and%20transaction%20costs%20-%20full.pdf.

right and the right of communication to the public (and/or the right of making available to the public): both have been harmonised under the Information Society Directive.[8] The CISAC decision and judgements concern the collective management of the so-called 'performing rights'. 'Performing right' is an industry term corresponding to the right of communication to the public and the right of public performance.[9] The right of reproduction is, within the media industry, typically referred to as 'mechanical right'.[10] Both rights are needed for most of the technology-related means of exploitation, and in particular for the online use. The distinction between mechanical and performing rights is nevertheless relevant in the context of licensing, as those two types of rights might be held by different right holders and may follow different licensing methods: i.e. the performing rights are typically managed collectively by the societies, but the mechanical rights in the so-called Anglo-American model of licensing are assigned by authors to their publishers who become the right holders of such rights.

Despite harmonisation, it is still the national laws which defines, for a given national territory, the exclusive rights in question and the scope of their protection. This also means that the exclusive rights need to be cleared for each of the national territories on which such rights are to be exploited.[11]

Unlike substantive copyright, the licensing and management of rights are barely regulated at international or EU level. The notable exceptions are the provisions of the Satellite and Cable Directive[12] providing for a compulsory collective management re-

8 European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, pp. 10 – 19, (referred to as 'Information Society Directive').

9 The latter has not been harmonised on the European level, this right however is of little relevance in the context of exploitation of copyrighted works by new technologies which is the core of the CISAC case. For industry definition of performing right see also CISAC decision, note 16.

10 See case COMP/M.3333 - SONY/ BMG, Commission decision of 3 October 2007, which in paragraph 627 defines the mechanical rights as rights for reproduction of a work in a sound recording.

11 Copyright is an amalgamation of rights granted to authors by various national laws. This is often referred to as the principle of copyright territoriality. The principle of territoriality is enshrined in Article 5(2) of the Berne Convention on the protection of literary and artistic works, signed in September 1886 . The CJEU has expressly confirmed the territorial nature of copyright in its Lagardere judgement (Case C-192/04, Lagardère *Active Broadcast v. Société pour la Perception de la Rémunération Équitable (SPRE) and Gesellschaft zur Verwertung von Leisungsschutzrechten mbH* [2005], para 46.). See also In: Derclaye, E. le (ed.), *Research handbook on the future of the copyrigh*, Edward Elgar Publishing, p.20.

12 Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and related rights of copyright applicable to satellite broadcasting and cable retransmission, OJ L 248, 6.10.1993, pp. 15-21, (referred to as 'Satellite and Cable Directive').

gime for cable retransmission,[13] and allowing Member States to provide for extended licensing in case of satellite broadcast.[14] The provision with particular impact on the licensing of communication to the public rights by the satellite broadcast is the so-called 'country of origin' rule of the Satellite and Cable Directive. Under the 'country of origin' rule the authorisation provided for a single national territory where the act of communication to the public takes place has a multi-territorial effect (covering the whole satellite footprint) in a sense that no separate licence is required for territories of other Member States where the satellite signal could be received.[15] Despite those few provisions of the EU directives, the rights management is largely left to regulation on national level and to private agreements between the right holders, the collecting societies, and the users.

The European institutions expressed their dissatisfaction with the inefficiencies of collective rights management in EU on several occasions, and called for development of multi-territorial licensing and greater transparency of the management process. To address some of the drawbacks of territorial collective management, and to improve the right's clearance within the EU, in 2005 the European Commission issued a Recommendation on the collective cross-border management of copyright and related rights for legitimate online music services.[16] The 2005 Recommendation aimed to encourage multi-territorial licensing of music for online use. According thereto, the right holders should be free to withdraw their rights from the local society and entrust the management of their online rights, with the territorial scope of their choice, to any collective management society of their choice, irrespective of residence and/or nationality of both the right holder and the societies concerned.[17] The Recommendation also promotes the possibility of direct licensing of online music, including for multi-territorial use. Following the 2005 Recommendation, music publishers decided to take full control of their mechanical rights in the Anglo-American repertoire, and withdrew them from the network of reciprocal representation agreements in order to license them directly: the publishers started to license such rights in collaboration with one or several pre-selected collecting societies which act as agents for publis-

13 Article 9 of the Directive.

14 Article 3 (2) of the Directive.

15 Article 1 point 2 (b) of the Directive, stating: «*The act of communication to the public by satellite occurs solely in the Member State where, under the control and responsibility of the broadcasting organization, the programme-carrying signals are introduced into an uninterrupted chain of communication leading to the satellite and down towards the earth*».

16 Commission Recommendation of 18 May 2005 on the collective cross-border management of the copyright and related right for legitimate on-line music services (2005/737/EC), OJ L 276/54, 21.10.1005 (referred to as 'the 2005 Recommendation').

17 See especially point 2, 3 and 5 of the 2005 Recommendation.

hers' rights (e.g. CELAS –a joint venture between the PRS of the UK and GEMA of Germany– acting for EMI Music Publishing; or the Pan European Digital Licensing (PEDL) – initiative of Warner Chappell, appointing several collecting societies in parallel as its agents). The withdrawal of mechanical rights by the publishers initiated the process of fragmentation of the right and of the repertoires: the global blanket licence covering the totality of copyrights (performing and mechanical) was no longer available at the local collecting societies.[18] The Recommendation was also criticized for lack of democratic legitimacy (due to the fact that it was not subject to the democratic legislative procedure).[19]

3. JUDGEMENTS AND DECISIONS IN THE FIELD

3.1. Competition Law Judgements

The Court of Justice of European Union (CJEU) has a long list of judgements where it considered the legality of contractual arrangements regarding copyright resulting in artificial partitioning of the market along national borders under European competition law. Already in *Coditel II*[20] the CJEU said that neither the copyright itself, nor the authority to territorially divide the mandates as such are subject to the prohibition of Article 101 TFEU[21] (then Article 85 of EC Treaty).[22] However, the CJEU did not excluded that «exercise» of the copyright by means of exclusive contractual arrangements to show the movie in one Member States for the specified period of time may come under prohibition of competition law rules «where there are economic or legal circumstances the effect of which is to restrict film distribution to an appreciable degree or to distort competition on the cinematographic market, regard being had to the specific characteristics of that market».

One of the subsequent judgements concerned the dispute between discotheque owners and the French collecting society Sacem.[23] Discotheque owners claimed that

18 The fragmentation of right remains the biggest problem for the licensing of copyright, in particular for online exploitation.

19 See European Parliament, Resolution of 13 March 2007 on the Commission Recommendation of 18 October 2005 on collective cross-border management of copyright and related rights for legitimate online music services (2005/737/EC), P6_TA(2007)0064, Strasbourg.

20 Case 262/81 *Coditel SA, Compagnie générale pour la diffusion de la télévision, and others v Ciné-Vog Films SA and others* [1982], (Coditel II), paragraph 17.

21 Treaty on the Functioning of the European Union, consolidated version, OJ C 326, 26.10.2012.

22 Treaty establishing the European Community, consolidated version OJ C 321E, 29.12.2006.

23 Case 395/87 *Ministère Public v. Jean-Louis Tournier*, supra *note* 1.

Sacem imposed excessive and unfair conditions, in particular excessive royalty prices. Discotheque operators had to pay high royalties to access the whole Sacem's repertoire. Sacem refused to grant access to just a part of its repertoire. Neither could the discotheques deal directly with the copyright management societies in other countries: the latter were bound by 'reciprocal representation contracts' with Sacem and –accordingly– refused to grant direct access to their repertoires. The national court referred several preliminary questions to CJEU, including the question on legality under the EU law of the organisation by the societies of a network of reciprocal representation agreements and these societies' collective practice of refusing to grant any access to their respective repertoires to users established in other Member States. As Advocate General Jacobs[24] stated:

> «The cases are highly unusual ones. At first sight, we are confronted with an absolute exclusivity de facto, a total compartmentalization of the common market within national frontiers, and a complete absence of competition, all of which would, in any other sector, be manifestly incompatible with Article 85(1). On the other hand, the market is a wholly exceptional one, because of the unusual nature of the intellectual property rights in question, which are not only territorial in scope, regulated exclusively by national laws differing significantly among themselves, and incidentally subject to very long periods of protection, but which also require continuous supervision and management within the national territories if they are to be effectively exercised.»

In its judgement, the CJEU concluded that reciprocal agreements are not themselves restrictive of competition. They might be caught by Article 101(1) TFEU if such agreements establish exclusive rights whereby societies do not directly license their repertoires cross-border, unless such can be explained by the objective reasons. The Court pointed that the need for local management and monitoring might justify such practice.[25]

3.2. Antitrust decisions

It is also noted that the Commission adopted a number of decisions concerning territoriality of licensing practices by collective societies when it reviewed the notifications of the so-called Simulcasting and the Cannes Extension Agreements. Those notified agreements were the model representation agreements the societies were concluding with each other for licensing of, respectively, the mechanical right for simulcasting, and the mechanical right for recordings. The agreements provided that a given collecting society was to licence the (combined) rights multi-territorially, but only for the users domiciled in its domestic territory. The Commission accepted these agreements, but only

---

24 Opinion Advocate General Jacobs in Case 395/87 *Ministre Public v. Jean-Louis Tournier*, delivered on 26 May 1989, paragraph 33.

25 It is noted that in recent judgement in case C 351/12 *OSA - Ochranný svaz autorský pro práva k dílům hudebním o.s. contre Léčebné lázně Mariánské Lázně a.s.* [2014] CJEU accepted that the local monitoring and protection of rights (in of-line context) might constitute the justified exception to the freedom to provide services as guarantied by Article 56 of TFEU.

after the societies abolished the customer allocation mechanism therein, and introduced the minimum price competition between societies for multi-territorial licences.[26]

Finally, in its recent *Premier League* judgement,[27] the CJEU also held that a system of exclusive broadcasting licenses which creates absolute territorial exclusivity in a Member State by prohibiting the sale of decoder cards to foreign television viewers, and by which the right holders partitioned the market with the aim of creating artificial price differences between Member States and thereby maximising profits (price discrimination) is contrary to EU internal market rules and EU competition law.

Territorial exclusivity was also at the heart of the CISAC case, which is discussed in detail below

4. THE CISAC DECISION

4.1. General

The European Commission adopted the CISAC decision on 16 July 2008.[28] The decision is addressed to 24 collecting societies operating in Europe, all associated with CISAC. The Commission finds that collecting societies infringed the EU competition law by including, in their reciprocal representation agreements, two infringing clauses, i.e. (i) the membership clauses, preventing the authors and other right holders to freely choose their collecting society, instead compelling them to become members of the society of their country of residence, and (ii) exclusivity clauses, by which societies grant each other exclusive mandates to license their repertoires. The CISAC decision finds the above mentioned clauses to be in breach of EU competition law and orders societies to remove them from reciprocal agreements.[29] Finally, the decision prohibits a concerted practice adopted by all concerned collecting societies with respect to the territorial

26 Under the original terms of these two agreements a single society was mandated by all other societies to grant multi-territorial and multi-repertoire licences, but only for the users established within the domestic territory of the given society. As both agreements have been subject to the Commission's review under the competition rules (Case COMP/C2/38.014 –IFPI «Simulcasting», Commission decision of 8 October 2002, and case COMP/C2/38.681 –The Cannes Extension Agreement, Commission decision of 4 October 2006) the Commission imposed their changes and elimination of the customer allocation mechanisms. The commercial user could then freely chose which of the EEA societies would grant him the licence covering the several territories. To protect authors' income, the competition was limited only to the administration fees charged by the societies or the margin of the wholesale price charged (the wholesale price itself being set).

27 Joined Cases C-403/08 and C-429/08, Football Association Premier League Ltd [2011].

28 See supra, *note* 1.

29 Articles 1-2 of the CISAC Decision.

delineation of the licensing mandates, which resulted in users being able to obtain the copyright clearance only for one domestic territory of each society concerned. The decision concludes that the concerted practice is restrictive of competition and orders the societies to enter into the bilateral re-negotiations of the reciprocal agreements with regard to the territorial delineation of the licensing mandates.[30] The latter two restrictions, i.e. the exclusivity clauses and the concerted practice, are of particular interest as they directly relate to the question of legitimacy of territorial restriction in copyright licensing.

4.2. Exclusivity clauses

Under the exclusivity clauses in the reciprocal representation agreements, the society was mandating its sister society to manage its repertoire «in the territories on which the latter society operates» on an exclusive basis. This territory of operation of the mandated society in question was typically defined as the national territory of the Member State where the society was incorporated. Such contractual exclusivity precluded the same national repertoire being mandated by more than one society per territory. The exclusivity clause also prevented the mandating society from licensing its own repertoire directly on the territory of its sister (mandated) society. As a result, societies have reciprocally guaranteed to each other the monopoly in their domestic territories.

4.3. Concerted practice of territorial delineation of mandates along national borders

According to the Commission, the collecting societies concerted with respect to the way they defined the territorial scope of the licensing mandates they granted each other in the reciprocal representation agreements. The Commission observed that all societies uniformly defined the scope of the mandates in question as limited to the domestic territory of each of the societies. Such parallelism of behaviour, according to the Commission, was indicative of concentration, as there was no alternative explanation, i.e. it could not be the societies' autonomous behaviour adopted in reply to the normal competitive market conditions.

In its assessment, the Commission distinguished between different types of exploitation of music and different technologies. The Commission established the existence and the anticompetitive effects of the concerted practice only in relation to licensing the satellite broadcast, cable re-transmission and online services, hence in relation to the technologies allowing for multi-territorial exploitation of music. In contrast, the Commission's finding of the concerted practice does not refer to other means of exploitation (local public performances, terrestrial broadcasts, etc.).

30 Articles 3-4 of the CISAC Decision.

The Commission concluded that, for those three multi-territorial means of exploitation, the systematic and uniform territorial delineation of mandates by national territory are neither necessary for the system of the reciprocal agreements to function, nor it could be justified on certain objective ground (e.g. such as requirements of the copyright law or cultural grounds). It results in the territorial segmentation of EU market into national monopolies: the cumulative effect of the systematic and uniform[31] delineation of mandates by the societies was the same as if there was the *expressis veribis* territorial exclusivity: there was only one source of licensing of the relevant rights in a given national territory. Hence it amounts to a concentration infringing Article 101 of TFEU. As the concerted practice results in the collecting society's inability to offer administration services and multi-repertoire licence beyond its own territory, the concerted practice eliminates entirely the competition in the markets for the administration of rights and the market for licensing the repertoires for the commercial users, contrary to the last condition of the exemption under Article 101(3) of TFEU.

The CISAC decision finds that the exclusivity clauses and the concerted practice restrict competition between the societies on two separate markets: (i) the provision of copyright administration services for public performance the societies grant to each other, as well as (ii) on the market of licensing of public performance rights for satellite, cable and internet transmissions to commercial users.

5. THE JUDGEMENTS

All but two collecting societies, to whom the CISAC decision is addressed, as well as CISAC itself, appealed it to the General Court. The General Court thus heard 22 separate appeals[32] against the (same) decision and on 12 April 2013 granted 22 separate judgements.[33]

---

31 The Commission makes the distinction between the ability of the collecting societies to limit territorially the scope of their mandates in individual cases, and the parallel and systematic delineation of mandates applied in the reciprocal agreements. The Commission states that only the latter is subject to the prohibition under the CISAC Decision, the former remains the uncontested rights of the societies (CISAC Decision, paragraph 215). The Commission also assures that the existence and the cooperation among the societies via the reciprocal representation agreements are not called into question, but there are no indications that the (systematic) territorial delineation is a prerequisite for the reciprocal agreements to exist.

32 Twenty four societies were addressees of the Decision. All of them appealed, except BUMA (the Netherlands) and SABAM (Belgium). SGAE (Spain) appeal was dismissed as it was lodged out of time. CISAC brought its own separate appeal. That brings the number of cases in front of the General Court and number of resulting Judgements to twenty two.

33 Case T-392/08 *AEPI v Commission*; case T-398/08 *ZAiKS v Commission*; case T-401/08 *Teosto v Commission*; case T-410/08 *GEMA v Commission*; case T- 411/08 *Artisjus v Commission*; case

In 21 of those judgements the Court partially annulled the Commission's decision.[34] The Court upheld the Commission's findings and remedies as regards the membership and exclusivity clauses, thus confirming they incompatibility with EU competition law. The Court however, concluded that the existence of the concerted practice was not proven to the required legal standard, and annulled the decision on the related points. In contrast, in the STIM's (Sweden) appeal, the Court upheld the CISAC decision in its entirety: STIM did not raise the objection as to the existence of the concerted practice, but sought its justifications on certain objective grounds, namely on ground of protection of cultural diversity. In this sole judgement the Court considered the anticompetitive character of territorial delineations.[35]

5.1. Parallel behaviour as concerted practice

In 21 of the CISAC judgements the Court did not accept the Commission provided sufficient proof of existence of concerted practice. The Court reminded that, in procedures relating to the competition law infringements, it is necessary to take into account the principle of the presumption of innocence,[36] which is one of the fundamental rights and a general principle of the Union's legal order.[37] The Court further reminds that the mere parallel market conduct might be considered an infringement only if the Commission provides sufficient evidence to render implausible any explanation for parallel behaviour other than infringing concentration.

The Court was not convinced that any of the circumstances invoked by the Commission are conclusive of the societies acting in a concert as regard the national territorial limitation of the copyright performing rights for free modes of exploitation concerned.[38]

T-413/08 *SOZA v Commission*; case T-414/08 *AKKALA v Commission*; case T-415/08 *IMRO v Commission*; case T-416/08 *EAU v Commission*; case T-417/08 *SPA v Commission*; case T-418/08 *OSA v Commission*; case T-419/08 *LATGA-A v Commission*; case T-420/08 *SAZAS v Commission*; case T-421/08 *PRS v Commission*; Case T-422/08 *SACEM v Commission*; Case T-425/08 *Koda v Commission*; case T-428/08 *STEF v Commission*; case T-432/08 *AKM v Commission*; case T-433/08 SIAE *v Commission*; case T-434/08 *Tono v Commission*; case T-442/08 *CISAC v Commission*; case T-451/08 *Stim v Commission* (action dismissed). The cases arising out of the appeals were not joined due to confidentiality issues.

34 As all those 21 judgements are to large extend alike. For sake of simplicity, we take the case T-442/08 *CISAC v Commission* (referred to as 'the CISAC judgement') as a model.

35 Case T-451/08 *Stim v Commission*, further referred to as STIM judgement.

36 Resulting in particular form the Article 6(2) of the European Convention of the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950.

37 Paragraphs 93-99 of the CISAC judgement.

38 In particular the Commission invoked instances of societies' discussions and cooperation amongst themselves which, according to the Commission, demonstrate that the societies were

In consequence, the Court considered whether the existence of the concerted practice could be established merely on the ground of the parallel conduct.[39]

Due to the burden and standard of proof that applies in such circumstances, it was sufficient for the societies to merely provide plausible alternative explanation of the parallel behaviour. The societies argued that limiting the licensing mandates to one national territory was not a result of concentration, but a rational decision of each individual society, dictated *inter alia* by the need for the local presence to effectively monitor the exploitation of copyrights, including detecting the unauthorized use of musical works. According to the Court, such explanation cannot be dismissed by merely declaring, as Commission did in the CISAC decision, that the decision applies only to the lawful use of the musical works and thus piracy is out of its scope.[40] The Court notes that the decision does not explain how it is possible to separate auditing the lawful licenses versus combating piracy, neither it proves that the societies are not involved in a fight against piracy for the three modes of the exploitation concerned, or that it can be done remotely (in cost efficient manner). The Commission also failed to demonstrate that the societies, once becoming competitors, still retains incentives to cooperate with each other as regards combating piracy.

In consequence, the Court concluded that the Commission did not provided sufficient evidence to render implausible the explanation of the parallel behaviour putted forward by the societies, hence it did not prove to the required standard the very existence of the concerted practice. Such was sufficient for the court to annul the CISAC decision on related points. It needs to be noted, however, that the Court's reasoning is concentrating solely on the issue of the standard of proof of concerted practice. While the Court accepted the societies' explanation for parallel behaviour[41] as the CISAC

discussing and coordinating the delineation of licensing mandates for performing rights. That in particular relates to concluding by the societies in question the Santiago Agreement (which concerned multi-territorial licensing of performing right for online use, see Case COMP/C2/38126 –Santiago Agreement), as well as then abandoning the Santiago agreement (after the Commission raised its objections as to customer allocation mechanism), which both indicate that the Societies were discussing and coordinating the delineation of licensing mandates for performing rights. Moreover, despite the fact that certain societies have dropped the exclusivity clauses in their reciprocal agreements, the deletion of the exclusivity clauses did not resulted in any material change in the behaviour of the societies as regards the management and licensing of the performance rights.

39 When the proof of concentration is based not only on the parallel behaviour but also on documentary evidences which shows that market practices in question were the result of concentration, the burden is on the undertakings concerned to challenge the facts indicating concentration employed by the Commission. See recital 99 of the CISAC judgment.

40 Recital 11 of the CISAC decision.

41 *Implicite* accepting the defences based on the need of effective protection of copyright.

judgements themselves cannot be thus interpreted as Court's positive statement as to societies' role in detecting and combating illegal exploitation of copyright, in particular as regards the three modes of exploitation in question. The Court is also silent as to the competitive assessment of the territorial delineations or their potential justifications.

5.2. Competitive assessment of territorial limitations

As regards the exclusivity clauses, none of the societies has actually challenged them in their appeals. Hence, the societies accepted their anticompetitive character. As regards the concerted practice, the Court found that it has not been proven to the required standard, and annulled the decision on related points without considering impact of the concerted practice on competition. The STIM appeal and STIM judgement differs in that respect. STIM in its appeal did not contest the Commission's finding as to the existence of the concerted practice. Hence, in that case the Court simply accepted the existence of the concerted practice has been established and proceed with the assessment of the Commission's reasoning as regards its anticompetitive character.

STIM essentially raised one single plea in law to contest the Commission's prohibition of concerted practice, that it is claimed that the Commission infringed Article 151(4) of the EC Treaty (now article 167(4) TFEU) by not appropriately assessing impact of its decision on cultural diversity.[42] Article 151(4) required the Community to take the cultural aspects into account in actions it takes under the Treaty, in particular in order to respect and to promote the diversity of its cultures.

STIM claimed that the traditional model of reciprocal agreements benefited cultural diversity as small and less profitable repertoires were always included into the global license, easily available to all music users from the local society. The global license was a result of the old system of reciprocal agreements and their national territorial limitations. Breaking that systems would lead –STIM claimed– to the collapse of the global license (fragmentation of repertoires) and consequently to the marginalization of niche repertoires. The Court noted, however, a strong connection between the fragmentation and the increased direct licensing. The later was made possible due to the removal of the exclusivity rather than the prohibition of the concerted practice. The societies could find the model of multi-repertoire licensing which is not based on territorial limitations: according to the Court the national territorial limitations are not a prerequisite of the cooperation between societies for sake of entrusting each other with repertoires and thus allowing for multi-repertoire licensing. Hence, according to the Court, the presence of the territorial limitations in all reciprocal agreements cannot be considered as objectively necessary or inherent to the protection of copyright. [43]

42 Paragraph 61, STIM judgement.

43 Paragraph 92, STIM judgement.

6. DEVELOPMENTS AFTER CISAC

The Commission's CISAC decision, in consequence to ordered the societies to remove the membership and exclusivity clause form their reciprocal representation agreements, as well as to re-negotiate the territorial delineation of their licensing mandates. Since the Commission imposed the obligation to renegotiate the reciprocal agreements on a strictly bilateral (hence confidential) basis, there is no transparency as to the results of such exercise. Few observations, however, can be made.

First, certain collecting societies took this opportunity to change their mandating strategies, and are more active in direct licensing of their own repertoires for multi-territorial users. For example, the PRS for Music, the UK collecting society, is actively licensing its performing rights alongside the rights in Anglo-American repertoires entrusted to it by certain publishers across all European territories. It is also known that certain other alliances between the societies and publishers are constructed. This marks the change from the local licensing of the global and blanket repertoire to the multi-territorial but mono-repertoire licensing by the societies. In a way, such development mirrors the earlier changes in the licensing of the mechanical right by the publishers.

Secondly, one could observe stronger regional initiatives for the licensing of rights: most notably the NCB (Nordisk Copyright Bureau) for the Nordic and Baltic region. NCB was originally established for the sake of facilitating the licensing of the mechanical rights for the region in question. The NCB grants one single licence covering the whole territory of participating societies.[44] Recently, the NCB members also use the NCB facilities to facilitate granting the licences for the performing rights. Another example is ARMONIA, an association of the Spanish, French and Italian collecting societies for authors composers and music publishers (SGAE, SACEM, SIAE) which coordinates the licensing of performing repertoires of the three societies as a single bundle for online and mobile exploitation as well as Anglo-American works of Universal Music Publishing and Latin works of Sony/ATV, EMI music publishing and Peer Music, on the basis of the mandates entrusted to them by said publishers.

In 2012, the Commission presented a proposal for a Directive on collective management of copyright and related rights (CRM Directive).[45] The Directive was subsequently adopted in February 2014, requiring transposition by Member States by April

44 KODA (Denmark), STEF (Iceland), STIM (Sweden), TEOSTO (Finland), TONO (Norway), LATGA-A (Lithuania), AKKA-LAA (Latvia) and EAU (Estonia).

45 Proposal for a Directive of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market, COM(2012) 372/2 final, 2012/0180 (COD), available at: http://ec.europa.eu/internal_market/copyright/docs/management/com-2012-3722_en.pdf.

2016.[46] The CRM Directive aims at improving governance and transparency of all collecting societies, and at facilitating multi-territorial licensing of music copyright. The latter is to be achieved by voluntary re-aggregation of repertoire around societies willing and able to license copyright on a multi-territorial basis. Only the societies fulfilling certain criteria (e.g. relating to their technical and organisational capacities) can grant multi-territorial licences. The society meeting such criteria and which accepted the repertoire from at least one other societies for multi-territorial licensing, is under obligation to accept the repertoire of other societies for licensing. Finally, the CRM Directive provides that a collecting society which does not engage in multi-territorial licensing of on-line rights must allow its authors to do so by other means, e.g. by using in parallel another collecting society for these purposes. Hereby, it aims at creating competitive pressure on societies to develop more efficient licensing practices.[47]

7. CONCLUSIONS

The general Court's judgements on CISAC decision has been often read as the victory of the traditional territorial model of licensing. It is submitted, however, that the judgements themselves –largely focused on the question of standard of proof of the concerted practice– are far from being conclusive as to the Court's approval of the territorial restriction in licensing. While the Court accepted that fight against piracy (i.e. the necessity of monitoring the illegal use on territorial basis) might constitute the plausible explanation for the parallel behaviour, it did not however concluded whether the collective management indeed undertakes such functions. The judgements are also inconclusive as to whether the need for local presence is necessary element of the reciprocal representation agreement and hence constitutes an objective justifications for territorial partitioning of the market. The Court accepts the local monitoring and fight against piracy as potentially relevant issue (it concerns the protection of Intellectual property and hence could in principle be accepted as justifi-

46 Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market, OJ L 84, 20.3.2014, pp. 72-98 (further referred to as 'CRM Directive').

47 Ccomprehensively on the proposal: Quintais, J. P. (2013). Proposal for a Directive on collective rights management and (some) multi-territorial licensing. *European Intellectual Property Review*, No 35 (2). 65-73.
Moscibroda, A. (2013). Collective rights management and multi-territorial licensing: the Commission's proposal for a Directive. *Auteurs & Media (A&M)*, issue 3-4/2013, 278 – 287. As regards discussed points, the CRM Directive (as adopted) does not significantly differs from the original proposal.

cation of competition restriction),[48] however the necessity and proportionality of particular societies' behaviour (i.e. systematic and uniform territorial delineations) would be subject to scrutiny (i.e. assessed against market realities). In the STIM judgement, the Court clearly stated that territorial limitations cannot be considered as objectively necessary and inherent in the protection of copyright, shows that any claim made by the societies to justify the territorial monopoly must be duly justified, in particular for those types of exploitations that are of multi-territorial nature. In any case, the Court confirmed that the practices of collecting societies are susceptible of the review by the Commission on competition grounds.

Finally, the CRM Directive clearly aims at encouraging the multi-territorial and multi-repertoire licensing. While the CRM Directive does not contain the prohibition of territorial (national) licensing, it indirectly imposes the obligation on society to licence directly its repertoire on multi-territorial level or to entrust other society with multi-territorial mandate for its repertoire. Hence, as practice of systematic territorial restriction in the licensing mandates of collecting societies seems to run against the aims of the new CRM Directive, the competitive assessment of such practices under the new Directive is likely to be more severe.

8. BIBLIOGRAPHY

European Parliament (2007). *Resolution of 13 March 2007 on the Commission Recommendation of 18 October 2005 on collective cross-border management of copyright and related rights for legitimate online music services* (2005/737/EC), P6_TA(2007)0064, Strasbourg.

Frabboni, M., (2009). Collective management of copyright and related rights: achievements and problems of institutional efforts towards harmonisation. In: Derclaye, E. le (ed.), *Research handbook on the future of the copyright*», Edward Elgar Publishing.

Hugenholtz, B, (2009). Copyright without frontiers: the problem of territoriality. In: European Copyright law. In: Derclaye, E. le (ed.), *Research handbook on the future of the copyright*», Edward Elgar Publishing.

48 Recent OSA judgment (see supra note 21) seem to indicate the CJEU, –given current sate of the EU law– is sympathetic towards justification for granting territorial monopoly by the Member State to a particular society based on effective protection of rights,, as currently no other method grants the same level of copyright protection then local monitoring. However, it needs to be remembered that and the OSA case concerns the of-line exploitation of copyright, and it provides interpretation of the Article 56 TFEU (freedom to provide services), and that assessment in relation to multi-territorial (on-line) exploitation and on competition grounds might not be the same.

KEA European Affairs, (2012). *Licensing music works and transaction costs in Europe.*, KEA, http://www.keanet.eu/docs/music%20licensing%20and%20transaction%20costs%20-%20full.pdf.

Moscibroda, A. (2013). Collective rights management and multi-territorial licensing: the Commission's proposal for a Directive. *Auteurs & Media (A&M)*, issue 3-4/2013, 278-287.

Quintais, J. P. (2013).Proposal for a Directive on collective rights management and (some) multi-territorial licensing. *European Intellectual Property Review*, No 35 (2). 65-73.

Uchtenhagen, U., (2011). Copyright Collective Management in Music. Geneva: WIPO.

Legal Acts:

- The Berne Convention on the protection of literary and artistic works, signed in September 1886.
- European Convention of the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950.
- Treaty establishing the European Community, consolidated version OJ C 321E, 29.12.2006.
- Treaty on the Functioning of the European Union, consolidated version, OJ C 326, 26.10.2012.
- Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and related rights of copyright applicable to satellite broadcasting and cable retransmission, OJ L 248, 6.10.1993, pp. 15-21.
- European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, pp. 10 – 19.
- Commission Recommendation of 18 May 2005 on the collective cross-border management of the copyright and related right for legitimate on-line music services (2005/737/EC), OJ L 276/54, 21.10.2005.
- Proposal for a Directive of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market, COM(2012) 372/2 final, 2012/0180 (COD).
- Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market, OJ L 84, 20.3.2014, pp. 72-98.

Case law and decisions

- Case 262/81-Coditel SA, Compagnie générale pour la diffusion de la télévision, and others v Ciné-Vog Films SA and others [1982].
- Case 395/87 Ministère Public v. Jean-Louis Tournier [1989] ECR 2521.
- Case C-192/04, Lagardère Active Broadcast v. Société pour la Perception de la Rémunération Équitable (SPRE) and Gesellschaft zur Verwertung von Leisungsschutzrechten mbH [2005].
- Opinion Advocate General JACOBS in Case 395/87 Ministre Public v. Tournier, delivered on 26 May 1989.
- Joined Cases C 403/08 and C 429/08, Football Association Premier League Ltd [2011].
- Case T-392/08 AEPI v Commission, [2013].
- Case T-398/08 ZAiKS v Commission, [2013].
- Case T-401/08 Teosto v Commission, [2013].
- Case T-410/08 GEMA v Commission, [2013].
- Case T- 411/08 Artisjus v Commission, [2013].
- Case T-413/08 SOZA v Commission, [2013].
- Case T-414/08 AKKALA v Commission, [2013].
- Case T-415/08 IMRO v Commission, [2013].
- Case T-416/08 EAU v Commission, [2013].
- Case T-417/08 SPA v Commission, [2013].
- Case T-418/08 OSA v Commission, [2013].
- Case T-419/08 LATGA-A v Commission, [2013].
- Case T-420/08 SAZAS v Commission, [2013].
- Case T-421/08 PRS v Commission, [2013].
- Case T-422/08 SACEM v Commission, [2013].
- Case T-425/08 Koda v Commission, [2013].
- Case T-428/08 STEF v Commission, [2013].
- Case T-432/08 AKM v Commission, [2013].
- Case T-433/08 SIAE v Commission, [2013].
- Case T-434/08 Tono v Commission, [2013].
- Case T-442/08 CISAC v Commission, [2013].
- Case T-451/08 Stim v Commission, [2013].

- Case C 351/12 OSA - Ochranný svaz autorský pro práva k dílům hudebním o.s. contre Léčebné lázně Mariánské Lázně a.s. [2014].
- Case COMP/C2/38126 –Santiago Agreement.
- Case COMP/C2/38.014 — IFPI «Simulcasting», Commission decision of 8 October 2002.
- Case COMP/C2/38.681 –The Cannes Extension Agreement, Commission decision of 4 October 2006.
- Case COMP/M.3333 - SONY/ BMG, Commission decision of 3 October 2007.
- Case COMP/C2/38.698 – CISAC, Commission decision of 16 July 2008.

A TALE OF TWO RIGHTS: MEDIATING BETWEEN P2P OWNERS AND DIGITAL COPYRIGHT HOLDERS

Bukola Faturoti
Senior Lecturer, The Law School
Aberdeen Business, School, Robert Gordon University [1]

ABSTRACT: The emergence of peer-to-peer file sharing technology revolutionises the discourse around copyright infringement. This new pirate of digital technology poses challenges not only to legal structures but it redefines tensions among various stakeholders: artists and creators genuine users of copyrighted works, content industries and technologists. They threaten cultural production turning users to consumers without effort to become producers. Conversely, it is contended that such software increase collaborative interactions and change the way we perceive social and communicative structures. A caveat is that the response of law when juxtapose with technological changes in the internet itself, has heavily increased the effective regulation of creativity. This paper examines the early debate around the regulation of p2p software. Can there be a middle ground?

KEYWORDS: Copyright, dual-use technology, authorisation, secondary infringement, peer-to-peer.

1. INTRODUCTION

Online sharing of music, sound recordings and videos have been caught between the battle for ownership and public right of usage. Technologies like peer-to-peer (P2P) which facilitate their communication and distribution have fallen under serious attack for being tools of commercial and non-commercial infringements yet they are capable of non-infringing purposes. The impact of P2P on music sales continue to be subject to constant debate. Forty billion files of copyrighted digital materials were alleged to have been shared illegally in 2008.[2] Such allegations have been contested as assertions

1 The author wishes to thank Thorsten Lauterbach of the Law School, Robert Gordon University for his comments and suggestions on earlier version of this paper. The author is grateful to Daniel Nikoi Kotei of University of Ghana whose opinions have also been useful while writing this essay.

2 IFPI, Digital Music Report 2009 available at http://www.ifpi.org/content/library/dmr2009.pdf accessed on 20 March 2014.

not based on statistically reliable information.[3] This paper re-examines the conundrum of online copyright infringement and P2P technology relationship. From Australian, American and Canadian perspectives, it investigates how courts try balance conflicting rights of technology developers and copyright owners. Does a constructive knowledge of infringing activities make an internet service providers or software manufacturer liable? How do courts strike a balance between the right of copyright holders interests and the needs of the society in encouraging technological innovation where software or material provided are *capable of commercially non-infringing uses* like time-shifting?

2. DUAL USE TECHNOLOGIES

P2P software technologies are not the first generation of dual-use technologies. Printing machines are the first known of dual use technologies which helped massive production of books, and other reading materials. These machines were good until they were used to print seditious materials or copyrighted materials without permission. More recent examples of dual use technologies are nuclear reactors that could generate plutonium for nuclear weapons and could also be used in generation of electricity and life saving pharmaceuticals.

Dual use technologies like VCR, internet, computer and p2p file sharing software have transformed the way we access and distribute materials. They allow a more democratic mode of publishing, free from state censorship and publisher monopolies. To copyright owners, these technologies are a destructive force to creativity.[4] Such criticism glosses over the contribution of these technologies in enhancing the popularity of creators through legal mass production and distribution of authors' works.

2.1. The nature of peer to peer technology

Though the popularity of term peer-to-peer could be attributed to Napster, the concept and technology which influenced P2P could be traced to older technologies like IP routers, Usenet news server system, FidoNet and others. These technologies moved towards distributed systems rather than monolithic systems.

Winer describes P2P as «a class of applications that take advantage of the resources –storage, cycles, content, human presence available at the edges of the

3 Marshall L, «Infringers» in Frith S and Marshall L (eds) *Music and Copyright* (Edinburgh University Press, 2nd ed 2004 p 194.

4 John Philip Sousa, «The Menace of Mechanical Music,» Vol. 8 (1906) *Appleton's Magazine 278-284.*

internet.»[5] A P2P as a network utilises the computing power and the bandwidth of the users in the network, each generally regarded as a peer. Each peer acts as a *servent* that is the nodes act at the same time as a client and as a server unlike a client-server networking, where the server has the responsibility for providing or serving network information and the client consumes or otherwise act as clients of those servers.[6] P2P networks do not have problems of scalability and redundancy. As participants on the network increase, the resource of the system also increases more so that every participant is both a provider as well as requestor.

P2P networks could be divided into two, namely those with a central entity and those without any central entities. A pure P2P network has no central server managing the network. Any single and arbitrary chosen peer can be removed without any disruption of the network service. Hybrid P2P networks on the other hand need a central server which maintains information on peers and responds to requests for such information. Some P2P networks use stronger peers called 'super-peers' or super-nodes' as servers; client peers are then connected to a single super-peer. Super-peers are decentralized networks because no specific machines serve as index servers. Instead the software running on all the peers takes stock of each other's available resources, including bandwidth, drive space, and processing power.

3. UNITED STATES COURTS AND DUAL USE TECHNOLOGIES

3.1. The Pre-Napster Approach

Under US copyright law, providers of technologies used for infringement could be held liable under the doctrine of secondary infringement (contributory infringement and vicarious liability). In respect of contributory infringement, «one who with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer.»[7] On the other hand, a manufacturer may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.[8]

---

5 David Winer 'Clay Shirky on P2P' available at http://scripting.com/davenet/2000/11/15/clayShirkyOnP2p.html.

6 Schollmeier R (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Proc. of 1st Intern. Conf. on Peer-to-Peer Computing, Linkoping, Sweden, pp. 101-102.

7 *Gershwin Publishing Corp. v Columbia Artists Management Inc.*, 443 F. 2d 1159, 1162 (2d Cir 1971).

8 Ibid.

In *Sony Corp. v. Universal City Studios, Inc*[9] the court sought to answer the question whether manufacturers of dual use technologies such as printing machines, photocopy machines and VCRs should be held liable for copyright infringements committed by users of their technologies. The plaintiffs alleged that Sony had contributed to infringement of its copyright by manufacturing and selling video cassette recorders (VCRs) which were being used by Sony's customers to infringe their copyrights in many motion pictures and television shows. It was led in evidence that Sony's advertisement encouraged users to record their favourite shows and build their own libraries.[10] The evidence also confirmed that some Betamax users had recorded and built libraries of television programmes produced by Universal Studios.[11] Sony argued that VCRs were «capable of commercially significant non-infringing uses», namely time-shifting of TV broadcasts.[12] It added that time-shifting was one of the fair usages contemplated under the US Copyright Act and more importantly the Congress had exempted private use of home recording from copyright violations. It would therefore be wrong for Sony to be held for infringements committed by VCR users merely because it sold the machine.[13]

The trial court ruled in favour of Sony but this was reversed by the Ninth Circuit.[14] That court rejected Sony's argument and held that time shifting of televised movies infringed Universal's copyright.[15] The court also held that the main aim of Betamax was to facilitate copyright infringement and Sony was aware of various acts of copyright violations being carried out by its customers.[16]

Dismissing the claims of the plaintiffs, the Supreme Court in its ruling acknowledged the necessity of balancing between the rights of copyright holders and the needs of society in encouraging technology. Justice Stevens explained that one of the duties of the Congress is to formulate a «difficult balance between the interest of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interest in the free flow of information and commerce on the other hand.»[17]

On liability for contributory infringement, the Supreme Court agreed that it may be manifestly just in some instances to impose secondary liability but constructive

9 464 U.S. 417 (1984).

10 Ibid at 459.

11 Ibid at 483.

12 Ibid.

13 Ibid at 447- 456.

14 *Universal Studios, Inc v. Sony Corp. of Am.,* 659 F.2d 963 (9th Cir. 1981).

15 Ibid at 971-972.

16 Ibid at 975-976.

17 Supreme Court at 429.

knowledge of infringing activity should not be imputed from a general awareness that a machine could be used for infringement. [18] The Supreme Court imported the «staple article of commerce» doctrine from patent law where a technology innovator would be contributory liable if his invention has been «especially made or especially adapted for use in an infringement of a patent.»[19] It would therefore be wrong to allow copyright owners to control the development of new technologies used in connection with copyrighted works. According to the court «the sale of copying equipment, like the sale of other articles of commerce does not constitute contributory *infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses*.»[20]

The decision in *Sony* established the fact that dual use technology owners would not be liable if they could prove that their technology is capable of substantial non-infringing uses even they have constructive notice of infringing usages. This decision paved ways for future development of other technologies that facilitate private and personal use copying.[21] However some bleak areas about the decision remained. It is not clear from the court's decision the importance it attaches or that should be attached to the word «substantial» when determining the quantum of infringement. Some authors concluded that the court erred by not putting its conclusion «capable of substantial non-infringement uses into context.[22] They explained that benefits derived from legitimate use should have been compared with harm occurring from illegitimate use. It appears that no matter the extent of copying, the owner of the technology would not be liable if it is private and there is no intention of any commercial benefit. The copyright holder must discharge the burden that such act of copying is harmful or that the widespread would have the market potential of the copyrighted work.

3.2. Liability of Peer-to-Peer Software Providers

It would seem obvious that the *Sony* decision has provided a safe harbour for makers of dual-use technologies. In 2000, A&M Records claimed that Napster through its P2P technology allowed its users to: (1) make MP3 music files stored on individual computer hard drives available for copying by other Napster users; (2) search for MP3 music files stored on other users' computers; and (3) transfer exact copies of the con-

18 Ibid 436.

19 35 U.S.C §271(c)(2000).

20 Note 8 at 442 (emphasis supplied).

21 Pamela Samuelsson The Generativity of S*ony v. Universal*: The Intellectual Property Legacy of Justice Stevens *Fordham Law Review* 2006 Vol 74 101-145.

22 William Landes & Douglas Litchman, «Indirect Liability for Copyright Infringement: An Economic Perspective,» *16 Harvard. J.L. & Tech (2003)* 395.

tents of other users' MP3 files from one computer to another via the internet.[23] Napster argued that activities of its users fell within the exception of fair use. The court held that the wholesale reproduction and distribution of copyrighted works by Napster users constituted direct infringement.[24]

On allegation of contributory infringement, relying on the decision in *Sony Corp v Universal City Studio,*[25] Napster argued that its facilities were capable of substantial non-infringing activities and it had no actual knowledge that its software was being used for infringing activities and if it had any notice it was a constructive one. The court agreed with the defendant on this point of law and explained that action premised on contributory liability would fail if it could not be proved that a manufacturer did more than 'merely supplying the means to accomplish an infringing an activity' and that the software was capable of commercially significant non-infringing activity. The court inferred actual and specific knowledge of direct infringements from the 12,000 copyright notices of infringing files supplied by RIAA and a document authored by a co-author of Napster on the «need to remain ignorant of users' real names and IP addresses…»[26]

Turning to the issue of vicarious liability, the defendant was also found liable for having a financial interest in the infringing activities and for failing to exercise its supervisory power in curtailing the activities. The District Court judge agreed that Napster software was capable of non infringing uses but held that the main aim of the software was to facilitate unauthorised copying and distribution of copyrighted songs.[27]

On appeal by the defendant, the Ninth Circuit dismissing the appeal expounded further that in the context of the copyright law, vicarious liability extends beyond an employer/employee relationship to cases in which a defendant «has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.»[28] The higher court agreed with the argument that the financial interest of Napster lied in the increases in the number of its base users and in fact more users did register as the quantity and quality of music increased.[29] The court varied the imposition of vicarious liability on the defendant on the ground that the district court failed to recognize that the boundaries of the premises that Napster «controls and patrols» are limited. » In other words Napster's reserved «right and ability» to police is cabined by

23 *A & M Records v Napster*, 114 F Supp 2d 896 CND Cal 2000.

24 Ibid at p 4427.

25 464 US 417 (1984).

26 A& M Records v Napster 2001 114 F Supp 2d 896 Napster.

27 Ibid 916-917.

28 Ibid (quoting *Gershwin*, 443 F.2d at 1162).

29 District Court's decision 114 F. Supp. 2d at 902.

the system's current architecture because the Napster system does not «read» the content of indexed files, other than to check that they are in the proper MP3 format.[30]

The Ninth Circuit gives *Sony* a narrow interpretation. It is doubtful if Sony's makers would have escaped liability as carved by the Ninth Circuit here because according to the court what the Supreme Court was guarding against was the imputation of constructive knowledge of another's party's infringement if the defendant was the maker of copying equipment capable of substantial non-infringing use. The opinion of Judge Bezzer suggests that more weight is placed on the sufficient notice. Though the court does not provide further explanation on the meaning of capable of substantial non-infringing activities, his analogy to computer network suggests that if the technology is capable of dual usages one of which is good the maker would not be liable except he engages in extra act which facilitates the infringement.

In *re Aimster Copyright Litigation*[31], the plaintiffs sought a preliminary injunction against the defendants for vicarious and contributory infringements.[32] The plaintiff alleged that the Aimster system proprietary software that can be downloaded free of charge from Aimster's Web site had been used in facilitating swapping of digital copies of music though Aimster did not make copies of the swapped files itself. It also provided computerized tutorials instructing users of the software on how to use it for swapping computer files; and formed «Club Aimster,» a related Internet service that users of Aimster's software could join for a fee and use to download the «top 40» popular-music files more easily.

The court held that the principle in *Sony* would not be applicable where the product was specifically manufactured for infringing activity even if the product was capable on non-infringing uses. Whether a technology is capable of substantial non-infringing uses or not would be irrelevant to the innovator's secondary copyright liability if the product's actual use was infringing.

On appeal, the Seventh Circuit affirmed the preliminary injunction solely on the contributory infringement claim and substantially narrower grounds. The court concluded that in applying the *Sony's* doctrine to the provider of an ongoing service, the provider's ability to supervise and prevent its customers from infringing is a vital condition to be considered in determining whether the provider is a contributory infringer. This ability to prevent should not form a sole factor in determining liability as this would have adverse consequences for the provision of dual services. The court explained that «if a service facilitates both infringing and non-infringing uses...and the detection and prevention of the infringing uses would highly be burdensome, the

30 Ibid.

31 334 F 3d 643 (7th Circuit, 2003).

32 252 F.Supp.2d 634.

rule could result in the shutting down of the service or its annexation by the copyright owners…»[33]

With respect to knowledge, the appeal court rejected the argument of the defendant founded on *Sony's case*[34] that «mere constructive knowledge of infringing uses is not enough for contributory infringement»[35] and that Aimster network traffic was encrypted and was thereby incapable of knowing exactly what files were being shared by individual end users.[36] In the lead judgement, Posner C.J. relied on *Casella v. Morris,*[37] and held that «[w]ilful blindness is knowledge, in copyright law.»[38]

Returning to the defendant's reliance on *Sony*, the higher court found that the defendant failed to demonstrate either in its pleadings or evidence that its software had been used for anything other than infringing activity. It however went to suggest that the application of the *Sony* case requires a consideration of the proportion of the infringing to non-infringing uses.[39]

This writer thinks that this decision conflicts with the Supreme Court's opinion as stated in *Sony.* The Seventh Circuit's decision underscores the continuing controversy whether the *proportion* of infringing and non-infringing uses is relevant to *Sony*. Though the Aimster's decision is more in tandem with the Sony's protection for providers of dual-use technology when compared with the decision by the Ninth Circuit in Napster, this interpretation creates a serious hurdle for innovation.[40] A provider of dual-use technology must take into cognisance whether non-infringing use of his technology will not only be substantial but whether it will be the primary use and whether either use could be substantiated in the court.[41]

Metro-Goldwyn-Mayer Studios Inc v Grokster[42] is important because (i) it was decided by the US Supreme Court; (ii) it acknowledged the *Sony* Safe harbour for technology providers; (iii) it introduced a copyright inducement liability and very importantly and; (iv)unlike other cases discussed above, the software was decentralised in nature.

---

33 Ibid at 649-650.

34 464 U.S. 104 S.Ct. 774.

35 Ibid at 439.

36 Ibid 651.

37 820 F.2d 362, 365 (11th Cir.1987).

38 Ibid.

39 Aimster Ibid.

40 Mark A. L*emley & R. Anthony Reese (2004) «Stopping Digital Copyright Infringement Without Stopping Innovation» Stanford Law Review* 56.

41 Ibid.

42 380 F 3d 1154 (9th Circuit, 2004); 545 US 913 (2005, US Supreme Court).

A consortium of entertainment companies led by Metro-Goldwyn-Mayer Studios Inc (MGM) brought an action for copyright infringement on the ground of contributory infringement against Grokster Ltd and StreamCast Networks, Inc.[43] According to the plaintiffs, the defendants knowingly and intentionally distributed their software to enable users to infringe copyrighted works in violation of the Copyright Act. The defendants did not contest direct copyright infringement by end users but counterclaimed that all they did was to connect all of the users of software into a network. Convinced by the arguments of the defendants, the trial court found them not liable for either contributory or vicarious copyright infringement.

The court, dismissing the appeal enumerated the principles contributory copyright infringement claim *viz.* (i) direct infringement by a third party (ii) knowledge of the infringement by the defendant (iii) material contribution to the infringement.[44] The first principle was not disputed by the parties. On the issues of knowledge, the court concluded that what the plaintiff must show is that the defendant had the actual and specific knowledge of the infringement; a constructive knowledge or mere awareness that end-users might use the technology to carry out infringement would not be enough especially in circumstances where it was also capable of non-infringing uses.[45] The plaintiff failed to establish this. Again, it was not proved that defendant could control the index files available for sharing; the network would operate even if the distributors withdrew from the network.[46] The Court of Appeal also found the defendant did not materially contribute to the infringement. It provided neither site (unlike Napster or Aimster) nor facilities for the infringement all it did was to make «a software» available.

Direct financial benefits to the defendant, the right and ability to control or supervise, and direct infringements are proofs to establish vicarious copyright infringement.[47] The court said that unlike Napster which has a central file server and could control access to it, neither Grokster nor StreamCast could search for infringing files or block the access to users. The defendants did not operate as a super-node, and the whole process of locating and connecting to a super-node occurred independently of them. It is erroneous to assume that the defendants have the ability to supervise or control the users. With this ruling we need to ask whether there could be liability for authorisation of copyright infringement as regards «decentralised» P2P network generally if a defendant proves that he cannot prevent infringement.

---

43 380 F 3D 1154 (9th Cir. 2004).

44 17 U.S.C.A 501- 513.

45 Supra note 192 at p 1160.

46 Ibid.

47 Ibid at 1164.

The Supreme Court, rather than addressing the issues of contributory and vicarious liability which were at the heart of the lower courts' decisions, propounded a new theory of copyright inducement of liability:

> «[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, going beyond mere distribution with knowledge of third part action, is liable for the resulting acts of infringement by third parties using the device regardless of device's lawful uses.»[48]

To determine the infringer's unlawful objective, it must be ascertained whether the alleged infringer: (a) showed itself to be aiming to satisfy a known source of demand of copyright infringement; (b) attempted to develop filtering tools or other mechanisms to diminish the infringing activity using the software or technology in question; (c) makes money by selling advertising space, by directing ads to the screens of computers employing their software.[49]

The apex court found that the defendants showed intent to foster infringing uses by targeting markets comprising former Napster users and the defendant failed to make any attempt to control end users' activities but engaged in active selling of spaces.[50]

On the issue of actual or constructive knowledge, Souter J clarified that the doctrine in *Sony* would not immunise someone who is seen to actively induce copyright infringement. According to him «*Sony* did not displace other theories of secondary liability and *Sony*'s rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires court to ignore evidence of intent if there is such evidence, and that the case was never meant to foreclose rules of fault-based liability derived from common law.»[51] The Supreme Court unanimously overruled the judgement of the lowers courts and remanded back to the District Court for disposition.

Is this the decision actually sought by the plaintiffs? Samuelson argued the actual winners are Grokster and other peer to peer developers because the court refuses to reverse or eliminate the safe harbour for technologies capable of substantial infringement non-infringing uses which was the actual aim of MGM.[52] She concluded that 'the copyright industry legal toolkit to challenge developers of p2p file-sharing technologies

48 *MGM Studios v Grokster Ltd* 125 S. Ct 2764 (2005) at 2770, 2780.

49 Ibid 2781-2780.

50 Ibid.

51 Ibid 2778-2779.

52 Pamela Samuelson, «Legally Speaking: Did MGM Really Win the *Grokster* Case?» Available at http://people.ischool.berkeley.edu/~pam/papers/CACM%20SCT%20decides%20MGM.pdf accessed on 23 March 2014.

is only marginally greater than before the Supreme Court decided the case.'[53] Therefore the decision of the Supreme Court did not actually translate into victory for digital copyright owners because it has actually deprived them what might be the strongest arguments in shutting p2p and other disruptive technology developers out of business.

4. FILE SHARING AND AUTHORISATION OF COPYRIGHT INFRINGEMENT IN AUSTRALIA

For a party to be liable of authorising an infringement of copyright there must have first occurred, «an act of infringement of the kind purportedly authorised.»[54] Ricketson explained that unless a person who performed an infringing act did it as an agent of the defendant, the defendant would not be liable.[55] Section 36(1A) of the Australian Copyright Act 1968 lists three factors upon which the liability of authorisation of infringement may be premised. The court must ask: (i) does the defendant have any power to control the infringement concerned; (ii) what is the nature of the relationship existing between the defendant and the direct infringer and (iii) has the defendant taken any reasonable steps to avoid the doing of the act, including whether the person complied with any relevant industry codes of practice?[56]

The case of *Moorhouse v University of New South Wales*[57] presents Australian courts position on balancing conflicting right of fair use and copyright ownership with dual use technologies. The plaintiffs had alleged that the defendant authorised massive infringement of copyrighted materials in which he has ownership outside the exemption of fair dealing for purposes of private study fair dealing and criticism. On 28 September 1973, Paul Brennan purposely copied some chapters from two books to gain evidence for the proceedings against University of NSW. The High Court asked the following questions (i) did Paul Brennan infringe the copyright of Mr. Moorhouse when he made those copies and (ii) if so, did the University authorise the act done by Mr. Brennan that infringed the respondents' copyright, namely, the making of the photocopies?

On the issues of authorisation, the court found the university liable on constructive knowledge of the act of infringement because if the University claimed that it did not know of infringements, there was ample evidence that it might have suspected

53 Ibid at p 1.

54 Lahore J and Rothnie WA, Copyright and Designs (Butterworth Lexis-Nexis online) at [34,095] http://www.butterworthsonline.com.

55 Ricketson, S; *The Law of Intellectual Property: Copyright Designs and Intellectual Property* (Lawbook Co., looseleaf service p 182).

56 ACA section 101(1A).

57 [1976] RPC 157.

it. Also, the University had failed to attach notices to the photocopy machines in a form prepared at the request of the Australian Vice-Chancellor's Committee. Placing of photocopier machines in the library without appropriate guidelines of terms of usage and adequate supervision is synonymous to invitation to copy. The notices placed in pursuance to s.49 of the Copyright Act by the university was applicable to photocopies made by and on behalf of the librarian and not to photocopies made by individuals for their own use. Absence of qualifying invitation might warrant indiscriminate copying by library users.[58]

This decision may be of limited application to liability of peer-to-peer file sharing technology providers. Much focus was on the compliance of the university with set of rules inviting users to make use of the machine. The caution which the American court emphasised on the dual-use technologies is absent. If the case applied to peer-to-peer file sharing the standard of supervision which the court places on providers might be too onerous. In a 'small' setting of the university, it is doubtful the level of supervision which a school can provide in monitoring materials being photocopied. The insufficiency of notices found by court is another strain. Factually, will hosting of billboards in a university library prevent illegal photocopying? The narrow approach in *Moorhouse* has largely influenced the peer-to-peer cases in the case below. What clearly follows is that activities which countenanced infringement either by omission or commission as in the American jurisdiction will be deemed as authorisation. This decision therefore shifts the balance in copyright too far in favour of the owner's rights and to the detriment of the proper use of copyrighted works for the good of the society as a whole.

4.1. Universal Music Australia Pty Ltd v Sharman License Holdings Ltd[59]

Universal Studios and 30 copyrighted music owners sued Sharman Networks; the manufacturer of the software, KaZaA,[60] for authorising illegal downloads of its copyrighted songs in contrary to the Australian Copyright Act.

The applicants claimed that the respondent, by offering for download to members of the public in Australia and by developing and maintaining technical distribution systems authorised the copying of whole or substantial parts of their copyrighted digital musical recordings without licence. The respondent contended that users of Kazaa and Altnet used a graphical user interface (GUI) which allowed them access to peer-to-peer

58 Margaret Jackson and Marita Shelly, «Black hats and white hats: Authorisation and Copyright Infringement in Australia and the United States» I.J.L. & I.T. (2006) 14(1), 28-46.

59 [2005] FCA 1242.

60 KaZaA is an internet peer-to-peer file sharing system which allowed users to exchange materials with one another irrespective of their location or distance to one another and whether or not the materials being exchanged are copyrighted.

network known as FastTrack. And FastTrack is content neutral software. There was no power or ability to control the files that users made available to each other or the content which they searched for or the content from which they made choices of downloads. Thus they did not authorise the alleged infringement acts but only conferred on users of the software the ability to make available for download by other users any file in digital format.[61] In its decision, the court found no liability on the claims but consider whether Sharman and its cohort were actually responsible for the authorisation of infringement committed by users of their software.

Section 112E provides that a person who provides facilities for making or facilitating the making of a communication is not taken to have authorized any infringement of copyright in an audio-visual item merely because another person uses the facilities to infringe copyright. The court was of the opinion that the exemption created by section 112E would not be available to a person where for reasons other than mere provision of facilities, he or she may have authorised the infringement in question. Wilcox J examined the non-exhaustive factors laid down in section 101(1A) and tried to strike a balance between the rulings of the court in *Adelaide Corporation v Australasian Performing Right Association Limited*[62]and *Moorhouse v University of New South Wales.*[63] It had been held in the latter case that authorisation can be made good *only* where it is established that the person has sanctioned, approved or countenanced the infringement. He thus concluded that authorisation here should not be narrowly construed as «express or formal permission or sanction»[64] rather it entails «inactivity or indifference exhibited by commission or omission.»[65]

In holding Sharman Networks Ltd liable of authorisation of infringing activities of end users, the found that the respondent had gone beyond mere provision of facilities «something more». There were series of positive conducts confirming authorisation (i) active promotion of its website as a file sharing facility and (ii) popularisation of unlawful file sharing by promoting the «Join the Revolution» movement. Furthermore, the respondents failed to install any sort of filtering devices despite their awareness of massive infringing acts.

---

61 The respondents like the defendants in Grokster highlighted the positive uses to which the software could be put. *There is a revolution underway which is changing the world of entertainment. It will effect how you discover, buy and share songs, movies, games and ideas. Peer-to-peer technology is driving the revolution and it could make life better for everyone. Lower prices, unlimited catalogs and more.»* See *Universal Music para 81'.*

62 [1928] HCA 10; (1928) 40 CLR 481.

63 [1976] R.P.C. 151.

64 Universal Music Ibid para 367.

65 Ibid.

5. GROKSTER AND SHARMAN COMPARED

5.1. Imposition of Liability

Decisions given by the US Supreme Court in Grokster's case and the Australian Federal Court in *KaZaA* agree that actions taken by the vendors of peer-to-peer file-sharing software might justify the imposition of secondary copyright liability for copyright infringement. Though the facts are seemingly similar, they the decisions are based on different factual merit and a different standard of liability. A direct infringement by the end-users is a common ground which all the cases recognise as a condition precedent for imposition of secondary liability. Before arriving at the liability of the producers, the cases conclude that there must be a primary infringement which is traceable to the software produced by the manufacturer. Mere production is not enough but there must be inducement or «something more.»

In *Grokster*, the U.S Supreme Court formulated a new theory of copyright inducement liability against third parties who produce and distribute devices capable of both infringing and non-infringing uses. This new theory is meant to complement the doctrines of contributory copyright liability and vicarious copyright liability. What this decision however suggests is that tangible evidence of actions motivating the use of the software for copyright infringement must be adduced.

Though the Australian court directed its mind to other inducements actions, this only formed one of the several elements the court considered in arriving at its decision. The court has been largely influenced by section 101 and 101(A) of the Australian Copyright Act. Section 101 imposes secondary liability on any person who, not being the owner of the copyright and without the licence of the copyright owner, authorises another person to do in Australia an infringing act.[66] Section 101(1A) provides further that regards must be had to «(a) the extent (if any) of the person's power to prevent the doing of the act concerned; (b) the nature of any relationship existing between the person and the person who did the act concerned; (c) whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.»[67] Also the court did not accept that section 112E on safe harbour as immunising against a liability for authorisation. Section 112 has excluded from liability a provider whose facilities have been used to violate copyright.

It is submitted that the decision in Australian's *KaZaA* is narrow compared to US *Grokster*. The Australian decision imposes a duty of care to adopt standards and provide

66 ACA 1968 s101(1).

67 *Copyright Amendment (Digital Agenda) Act 2000 Amendments* from Act No. 63 of 2002.

mechanisms for the prevention of copyright infringement on manufacturers and distributors of peer-to-peer file sharing software. This negligence-type rule holds providers of software liable for any failure to design any economically reasonable measures to prevent the harm of infringements.[68] Though the US Supreme Court settled for the theory of inducement, it does not mean the common law doctrine of secondary liability could not be shaped into negligence-type rule as did by the Australian federal court.[69] Apparently, the US court contemplated the side effects of secondary liability and such other factors like the fear that copyright owners might gain control over new and the budding technologies and the resultant effect of imposition of liability on manufacturers and distributors might have on non-infringing activities that rely on and use the same devices.[70]

By and large, *Grokster* protects distributors and manufacturers of peer-to-peer file-sharing software from secondary liability unless copyright owners discharge the burden of proof of inducement of copyright infringements engaged in. In *KaZaA* on the other hand, the duty of care standard has far reaching implications for providers of software. Is the *KaZaA* decision not over stretching the «neighbour test» and «reasonably foreseeable test» negligence doctrine of common law? What does this suggest to internet service providers who have no capabilities of taking reasonable step to prevent or control copyright infringements of peer-to-peer file sharing activity? A common conclusion of the court approach both the negligence rule and imposition of secondary liability save enforcement costs of suing a large number of end users who are engaging in primary infringement activity.[71]

Grokster did not discuss how contributory infringement and inducement of infringement liabilities might extend to joint venture parties. On the other hand the court in the *KaZaA* case adopted a wide approach and found liable other respondents who had real control or influence over policy making in the development and operation of the KaZaA system. These fringe players (controlling corporate shareholders and dominant sole directors) were liable individually and joint tortfeasors pursuant to a common design[72] of having the knowledge of end users infringing activities because despite their powers they failed to implement preventive measures or control the acts. This liability will exclude employees without any real say or influence in companies' policy making.

---

68 Guy Pessach, «An International Comparative Perspective on Peer-to-Peer File Sharing and Third Part Liability in Copyright Law: Framing the Past, Present, and Next Generations' Question» *Vanderbilt Journal of Transnational Law* Vol. 40 (2007) 1 at 7.

69 Supra note 21 at 405.

70 See Breyer J concurring opinion in *MGM Studios Inc v. Grokster Ltd.*, 125 S. Ct 2764, 2792-96 (2004).

71 Guy Pessach Note 67 at 8.

72 Sharman 2005 at para 489.

5.2. Knowledge

Generally, knowledge is a condition precedent for proof of liability under contributory infringement doctrine and inducement of infringement doctrine in the US. It was held in some cases that actual knowledge of specific infringement is required where the product is capable of substantial non-infringement and constructive knowledge suffices where the product is not capable of such uses. Elsewhere, proof of constructive knowledge by the defendant discharges the burden. It is unfortunate that US Supreme Court failed to stipulate the required form of knowledge. This has led to further contradictory interpretations by the lower courts. In the re-hearing of the *Grokster* case, Wilson J was of the opinion that what the Supreme Court suggested was that liability may attach if all the defendant had is constructive knowledge of the infringement.[73] However in *Monotype Imaging, Inc et al v Bitstream Inc*,[74] the court was of the opinion that *Grokster* precluded constructive knowledge.

The Australian court places less emphasis on the type of knowledge required. The court is of the view that there may be authorisation without knowledge and yet mere knowledge will not be enough.[75] It follows that knowledge forms one of the factors which Australian court will put into consideration and its absence would not be detrimental to proof of authorisation due to the negligence-type rule and the provision of section 101(1A) of the Australian Copyright Act as amended by the Digital Agenda Act 2000.

5.3. Safe Harbour

The importance of safe harbour is to exclude genuine providers and users from liabilities. Its purpose is to strike a balance between innovation and competition on one hand and copyright owners' interest on the other hand. The court in *Sony* stipulates what constitutes a defence to contributory infringement and section 112E prescribes a safe harbour under the Australian Copyright Act. *Sony* has excluded from contributory liability producers of product capable of substantial non-infringing uses. According to the court no liability would lie on presumption of intent to cause infringement solely from design or contribution of a product capable of lawful use. The US Supreme Court complicated issues by failing to address or expatiate on some elements which were not resolved in *Aimster* and the Court of Appeals' decision in *Grokster*. For example the Supreme Court could have defined 'capable of substantial non-infringing uses' and the

73 Actual transcript cited in Jeffrey C.J. Lee, «The ongoing Design Duty in Universal Music Australia Pty Ltd v Sharman License Holdings Ltd: Casting the Scope of Copyright Infringement Even Wider» *Int J.L. & I.T* (2007) 275 at 292.

74 Civ. No. 03 C4349 (N.D. 111, July 12, 2005).

75 Sharman para 370.

point at which contribution could be said to have occurred. When we say substantial, is it on quality or quantity?

Unlike the court in *Grokster*, the Australian court's approach though wide seems clearer. The court puts manufacturer and providers under a strict liability similar to the old English authority in *Ryland v. Fletcher*.[76] According to Wilcox J section 112E does not confer *general* immunity against a finding of authorisation' when for other reasons, the alleged infringer may have taken to have authorised the primary infringement. Two things come to mind when considering the court's interpretation of *s112E*. First, the court must have adopted the «mischief rule of interpretation» to make sure that *Digital Amendment Act* responds to the purpose of its enactment; to combat technological threat to IPR regime. Second, a defendant must really prove that he fits within the exception to invoke the safe harbour provision. Therefore a defendant must establish that there is no authorisation in any form. On the contrary, the defendant had an actual knowledge that the predominant use of the software was for sharing of copyright material.[77]

Casting the scope of secondary infringement wider, the Australian court failed to really define what would the safe harbour be. It failed to outline circumstances under which circumstances under which technology distributor may seek fortress of section 112E when confronted with liability from misuse of their of their products. Has the Australian court not rendered the section 112E safe harbour provision useless? Will such an approach not stifle technological development and innovation when the essence of copyright is to develop science and arts? There is little contention that the Australian approach is strictly pro-copyright protection.

6. PEER-TO-PEER FILE-SHARING IN CANADA – PURSUING THE INDIVIDUALS

The approach to liability of distributors of p2p software in Canada is pretty vague and most complex of all jurisdictions examined in this paper.[78] Canada is described as «a haven where technologically sophisticated international piracy organizations can operate with virtual impunity»[79] because it lacks controversial legislation like the American DCMA which expressly prohibits the breaking or the distribution of tools for breaking technology preventing piracy.

76 (1868) LR 3 HL 330.

77 Para 186.

78 International Intellectual Property Alliance Canada 2011Special 301 Report on Copyright Protection and Enforcement available at http://www.iipa.com/rbc/2011/2011SPEC301CANADA.pdf accessed 23 March 2014.

79 Ibid.

In the US and Australia, primary infringement by end-users set the ground for the secondary liability of the up-loaders and distributors of software. The Canadian copyright law allows making of a copy for personal use but fails to address the source of that copy. In the absence of specific legislation, the legality or otherwise of uploading will be in favour of end-users.

Section 80(1) of the Canadian Copyright Act excludes users from liability for downloading of musical works and sound recordings for private use purposes. If an end-user however copies a copyrighted work with the aim of selling or renting, distributing, communicating to the public by telecommunication or performing in the public according to s.80 (2) it shall no longer be deemed as private copying. The *Private Copying Decision*,[80] by the Canadian Copyright Board confirmed that private copying onto audio recording media by end-users is permissible but the liability of those uploading or providing software or operating networks or internet connection is not in issue.[81] It does not matter whether the source of the track is a borrowed CD or downloaded from the internet.[82] The Canadian Recording Industry Association (CRIA) alleged that some users infringed its copyright by illegally trading in music downloaded from the internet by means of KaZaA software. The Canadian Federal Court was invited in *BMG Canada Inc v John Doe*[83] to compel five Canadian ISPs to disclose the identity of these end-users. The court declared that «copyright law can be invoked by owners only to the extent explicitly set forth in the statute. A court cannot infer or provide right that are not provided for in the statute.»[84] Placing of a copy on a shared directory in a computer where that copy can be accessed via a P2P service does not amount to distribution.

On what might contribute authorisation, the court alluded to the Canadian Supreme Court's decision in *CCH Canadian Ltd v Law Society of Upper Canada*[85] where it was held that «a person does not authorise infringement by authorising the mere use of equipment that could be used to infringe copyright.» The court was of the view that rule of authorisation must be limited in scope particularly attention must be paid to the relationship or degree of control which exist between alleged authoriser and the person who committed the copyright infringement. On the legality or otherwise of P2P, it was held that such a decision should be left for the future. This over-cautious approach perpetuates the legal vacuum and ambiguity surrounding the Canadian approach to P2P music file sharing.

---

80 Private Copying 2003-2004 (Copying for Private Use (2003) available at http://www.cb-cda.gc.ca/decisions/c12122003-b.pdf accessed on 27 March 2014.

81 Ibid at p 19.

82 Ibid at p 20.

83 See also *BMG Canada Inc v John Doe* [2004] FC 488.

84 Ibid at 23.

85 [2004] SCR 339 at 38.

The CCH decision suggests that authorisation in Canada would also require active participation by inducer as found in earlier examined cases; and the control which the distributor could exercise on users and their activities. It is also clear that a user for private purpose must not distribute but the way P2P works does not require any action from a user before a recipient could have access to his shared directory. Can liability be imposed on a private user for not blocking access to his shared directory? That is, liability based on omission to act.

Cases such as *Voltages Pictures LLC v. Jane Doe*[86] and *NGN Prima Productions Inc v Does*[87] suggest that copyright holders prefer to pursue human distributors instead of technology developers. So the Canadian court has not properly had the opportunity to examine the nature of P2P technology. The *Demonoid's* owner shut down its system and later prevented access of downloaders with Canadian IP address.[88]There seems little doubt that this case may afford the court the opportunity create or follow the concept of capable of substantial non infringing uses.

7. CONCLUSION

This essay has retraced the interaction of P2P networks with copyright law. It establishes that a complex and interdependent relationship between copyright law and technology still exists. Copyright law provides an incentive for author to create new works and also gives the society the opportunity to have access to the information it needs. Peer-to-peer software revolutionises access and consumption of entertainment by snatching control of distribution away from the authors and creators. With the help of the court, copyright law is however expanding in determining the fate of technologies which are a tool which facilitates the dissemination of this information. Such expansion has been not a blanket or unbridled one as they are strictly regulated by the courts. The courts in the jurisdictions considered have used various factors among which are: the dual nature or the significance of non-infringing uses, absence or lack of intent in promoting infringement, the level of control on the use of technology, knowledge of infringement and the financial benefits to determine the extent of liability of technology owners. Comparing these decisions, it is obvious that finding a middle ground continues to remain blurry. The approaches in the US and Australia share some similarities while Canada offers something which is at the far end of the spectrum.

---

86 [2011] F.C.J. No. 1260 available at https://cippic.ca/uploads/Voltage_v._Does-2014FC161.pdf accessed on 20 March 2014.

87 Federal Court, Montreal Quebec November 19, 2012 available at http://copyrightenforcement.ca/wp-content/uploads/2012/11/NGN-Order-Montreal.pdf accessed on 20 March 2014.

88 Nick Farrell «Demonoid p2p site returns from dead» http://www.theinquirer.net/inquirer/news/1002844/demoniod-p2p-site-returns-dead accessed on 20 March 2014.

8. BIBLIOGRAPHY

A & M Records, Inc v Napster, Inc.,114 F Supp 2d 896 CND Cal 2000

A & M Records, Inc v Napster, Inc., 239 F.3d 1004 (9th Cir.2001)

A & M Records, Inc v Napster, Inc., 284 F.3d 1091 (9th Cir.2002)

Australian Copyright Act 1968 as amended

BMG Canada Inc v John Doe [2004] FC 488

CCH Canadian Ltd v Law Society of Upper Canada [2004] SCR 339 at 38

Copyright Amendment (Digital Agenda) Act 2000 Amendments from Act No. 63 of 2002

Gershwin Publishing Corp. v Columbia Artists Management Inc., 443 F. 2d 1159, 1162 (2d Cir 1971).

Farrell, N., «Demonoid p2p site returns from dead» http://www.theinquirer.net/inquirer/news/1002844/demoniod-p2p-site-returns-dead

IFPI, Digital Music Report 2009: New Business Models for a Changing Environment 2009 available at http://www.ifpi.org/content/library/dmr2009.pdf accessed on 20 March 2014

International Intellectual Property Alliance Canada 2011 Special 301 Report on Copyright Protection and Enforcement available at http://www.iipa.com/rbc/2011/2011SPEC301CANADA.pdf

Marshall L, (2004) «Infringers» in Frith S and Marshall L (2nd eds) *Music and Copyright* Edinburgh University Press

Lahore J and Rothnie WA, *Copyright and Designs* (Butterworth Lexis-Nexis online) at [34,095] http://www.butterworthsonline.com

Lee, J. C.J.«The ongoing Design Duty in Universal Music Australia Pty Ltd v Sharman License Holdings Ltd: Casting the Scope of Copyright Infringement Even Wider» *Int J.L. & I.T* (2007) 275 at 292

Lemley, Mark & Reese, A. (2004) «Stopping Digital Copyright Infringement Without Stopping Innovation» Stanford Law Review, 56.

Litchman, D., & William, L (2003) Indirect Liability for copyright infringement: An economic perspective 16 Harvard Journal of Law and Technology.

MGM Studios v Grokster Ltd 125 S. Ct 2764 (2005) at 2770, 2780

Margaret Jackson and Marita Shelly, «Black hats and white hats: Authorisation and Copyright Infringement in Australia and the United States» I.J.L. & I.T. (2006) 14(1), 28-46

Moorhouse v University of New South Wales [1976] RPC 157

Monotype Imaging, Inc et al v Bitstream Inc Civ. No. 03 C4349 (N.D. 111, July 12, 2005)

NGN Prima Productions Inc v Does Federal Court, Montreal Quebec November 19, 2012 available at http://copyrightenforcement.ca/wp-content/uploads/2012/11/NGN-Order-Montreal.pdf

Pessach, G., «An International Comparative Perspective on Peer-to-Peer File Sharing and Third Part Liability in Copyright Law: Framing the Past, Present, and Next Generations' Question» (2007) *Vanderbilt Journal of Transnational Law* Vol. 40, 1

Private Copying 2003-2004 (Copying for Private Use (2003) available at http://www.cb-cda.gc.ca/decisions/c12122003-b.pdf accessed on 27 March 2014

Ricketson, S; *The Law of Intellectual Property: Copyright Designs and Intellectual Property* (Lawbook Co., looseleaf service p 182)

Samuelsson, P., The Generativity of S*ony v. Universal*: The Intellectual Property Legacy of Justice Stevens 2006 Fordham Law Review Vol 74 101 – 145

Samuelsson, P., «Legally Speaking: Did MGM Really Win the *Grokster* Case?» Available at http://people.ischool.berkeley.edu/~pam/papers/CACM%20SCT%20decides%20MGM.pdf accessed on 23 March 2014

Schollmeier R (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Proc. of 1st Intern. Conf. on Peer-to-Peer Computing, Linkoping, Sweden, pp. 101–102,

Soussa, J. P., «The Menace of Mechanical Music,» (1906) Vol. 8 *Appleton's Magazine 278 – 284*

United States Copyright Act, 17 U.S.C.

Universal Studios, Inc v. Sony Corp. of Am., 659 F.2d 963 (9th Cir. 1981)

Voltages Pictures LLC v. Jane Doe [2011] F.C.J. No. 1260 available at https://cippic.ca/uploads/Voltage_v._Does-2014FC161.pdf

William Landes & Douglas Litchman, «Indirect Liability for Copyright Infringement: An Economic Perspective,» *16 Harvard. J.L. & Tech (2003)* 395 at 405

Winer, D., 'Clay Shirky on P2P' available at http://scripting.com/davenet/2000/11/15/clayShirkyOnP2p.html

6

GOOGLE NEWS AND COPYRIGHT EXCEPTIONS – WHERE DO WE STAND?

Marta Joanna Czeladzka (LL.M.)
PhD candidate
University of Warsaw

ABSTRACT: At the moment, no copyright statute refers to news aggregation. It is not surprising then that news aggregators present a challenge for any court having to deal with any aspect of their activity. Indeed, with any particular form of aggregation there are a number of competing interests at play: the copyright holder, the aggregator, the reader and the public at large. So far, there were only two suits against Google Inc. based on copyright infringement concerns from Google News, one in the US and one in Europe, but they revealed a lot of problems that existing copyright law may have with news aggregators. Assuming that Google News is involved in acts of exploitation of copyrighted works, the main issue the courts had to address when dealing with Google News was in fact the question whether any limitation/exception provided by copyright law had been applicable to this service. What can come into play in this regard are (1) the exception of quotation, (2) the exception for report on news events, and (3) the fair use defences. Failed to be allowed to rely on any of these exceptions, one may turn to other solutions, such as agreements between companies running aggregation sites and newspaper publishers (Belgium, France), governing the use of snippets of newspaper articles by news aggregators, or legislative measures in this regard (Germany). All this opens the discussion to touch the very concepts of law, and not only copyright law. It seems to that a balance will have to be reached in the near future juggling copyright protection, the function of news reporting (with public policy and fair use defence at stake) and freedom of speech in accessing and spreading the news. In reaching it, certainly not only copyright law, but also competition law and even human rights law issues will have to be examined.

KEYWORDS: Google News, news aggregator, copyright exception, fair use, licence.

1. INTRODUCTION

Google News, the biggest free news aggregator, provided and operated by Google Inc.[1], definitely represents one of the most interesting copyright-related series of cases over the last few years. Although it may seem small and not complicated service, Google News concentrates so many aspects that almost all vital problems of current copyright

1 Google News is available for more than 60 regions in 28 languages with continuing development ongoing.

law are in its orbit. As a result, Google has been involved in a set of court cases, as well it has become the crucial player for governments in a task of reshaping the balance between copyright protection and public interest in accessing and spreading the news.

It is because the operation of Google News –as any other aggregation site– is based on the use of third-party pre-existing contents that may be protected by copyright. Google News aggregates news articles appearing within the past 30 days on various news sites worldwide, groups similar stories together and displays them according to each reader's personalized interests, providing the readers with an array of stories from the day[2]. Yet, the vast majority of content used by this service is still provided by the traditional news formats. What is more, without the (pre-existing) content of news publishers, news agencies and broadcasters, Google News would make no sense at all.

Google does not edit the content aggregated. However, news are displayed not in the form of full articles, but instead in the form of a headline from news sources worldwide, the leading line from the original story, a photograph illustrating the news event being reported, and a link to where the full article can be viewed. Following the link, the user leaves the Google News website and is taken to the third-party website where the respective story or photograph is hosted and displayed.

Google's business model is based on a strategy to attract as much as possible of Internet traffic to websites of its own services and applications, in order to collect as much as possible information about its users. This information is essential for Google as it is used to personalize advertising. The more services provided by Google, the more websites there are to place sponsored links. The more sponsored links are clicked, the more revenues for Google[3]. Accordingly, launched in September 2002, Google News was intended as a specific application of Google's general search engine, an English-language 'news service' to complement company's offer to Internet users. Although, unlikely to other Google's products Google News does not contain any advertising, ads do appear after a user searches for content within Google News. Yet, it must be remembered that this free service can only be provided thanks to the significant revenue Google generates as a result of the attractiveness of all its services and the horizontal sliding of revenue which this interactivity facilitates.

Such a business model is in sharp contrast to the traditional media. During the past few years the Internet has become the most important news source for people all over

2 Stories to show are chosen automatically by Google's 'web crawlers' ('googleboots') that evaluate, among other things, how often and on what sites a story appears online. Other criteria are freshness, location, relevance and diversity.

3 Lopez-Tarruella A. (2012) Introduction: Google Pushing the Boundaries of Law, in: Lopez-Tarruella A. (ed.) Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, T.M.C. Asser Press, The Hague, The Netherlands, 5.

the world. Accordingly, the traditional media seem to be in retreat. It is claimed that Internet is harming the media business – the increased reliance on the Internet as a source of news has caused devastating income losses for traditional news business. Aggregation sites are identified as the main reason for this: news aggregators by –as they are being accused of– free-riding on factual information gathered by traditional media organizations get profits from them and contribute to the industry's decline[4].

Indeed, with any particular form of aggregation there are a number of competing interests at play: the copyright holder, the aggregator, the reader and the public at large. Google News entails unavoidable meeting of copyright and right to access to information that are both strong public interests. The very existing of news aggregators resets the issue of a delicate balance that needs to be drawn between the unquestionably beneficial informatory function that news aggregators provide to the Internet-using public and the potential impact those services have on right holders in the content to which those services eventually lead.

At the moment, no copyright statute refers to news aggregation. It is not surprising then that news aggregators present a challenge for any court having to deal with any aspect of their activity. So far, there were only two suits against Google Inc. based on copyright infringement concerns regarding Google News. The first claim, brought in 2005 in the United States, where the claimant Agence France Press alleged that Google was reproducing and publicly displaying AFP's photographs, headlines, and story leads on Google's news aggregation website without AFP's permission[5], resulted in a settlement (after two years in court)[6]. But the case brought against Google in Europe in 2006 by Copiepresse, the collective management organization for Belgian newspaper publishers in French and German languages, found that Google had infringed copyright law, as through its Google News service it reproduced and communicated to the public

4 Bunz M., Rupert Murdoch: 'There's no such thing as a free news story', The Guardian, 1 December 2009, available at: http://www.theguardian.com/media/2009/dec/01/rupert-murdoch-no-free-news, last accessed 1 May 2014.

5 Agence France Press v. Google Inc., No. 1:05-cv-00546-GK D.C.C. 17 March 2005, No. 1:05-cv-00546-GK D.C.C. 29 April 2005, No. 1:05-cv-00546-GK D.C.C. 19 May 2005, No. 1:05-cv-00546-GK D.C.C. 8 June 2005, No. 1:05-cv-00546-GK D.C.C. 12 October 2005, No. 1:05-cv-00546-GK D.C.C. 6 April 2007.

6 The parties entered into licensing agreement in 2007 that allowed Google to post AFP contents in full text (so not only snippets of articles but articles as a whole) on its sites. No further details were disclosed so it was not clear whether the deal involved a flat fee or paying AFP according to traffic statistics. In August 2006 Google forged a similar agreement with the Associated Press. McCarthy C., Agence France-Presse, Google settle copyright dispute, CNET News, 6 April 2007, available at: http://news.cnet.com/2100-1030_3-6174008.html?part=rss&tag=2547-1_3-0-20&subj=news, McCarthy C., Google Reveals payment deal with AP, CNET News, 3 August 2006, available at: http://news.cnet.com/Google-reveals-payment-deal-with-AP/2100-1030_3-6102109.html, last accessed 1 May 2014.

newspapers' copyrighted works[7]. Since the use of copyrighted works has been made by Google without asking copyright holders for their permission, the court came up with the idea of considering copyright exceptions as a way to justify its operation. Hence, the discussion about news aggregators fits very well with the ongoing debate on limitations and exceptions to copyright, as it has been submitted that due to the development of new technologies and the ever-increasing worldwide use of the Internet, the proper balance between various stakeholders' interests needs to be recalibrated.

This article aims at contributing to the discussion on how existing exceptions and limitations can fit with services such as Google News. The first section analyses the exception of quotation, and the second section –the exception for report on news events, with regard to Google News service. Then, the freedom of expression in the context of Google News service is discussed. The next sections address the application of *common law*'s *fair use* defence in the process of justifying the operation of Google News. Subsequently, assuming that news aggregators can hardly fit into existing copyright exceptions and limitations, it is considered whether any other approach to Google News could be implied, namely concluding agreements between companies running aggregation services and local newspaper publishers, governing the use of snippets of newspaper articles by news aggregators, or any legislative measures in this regard. Finally, some conclusions and possible further developments follow.

2. EXCEPTION OF QUOTATION

As regards exception for quotations, article 10(1) of the Berne Convention states that it shall be permissible to make quotations from a whatever work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries. Article 5(3)(d) of the Infosoc Directive states that Member States may provide for exceptions or limitations to the rights of copyright holders in case of quotations for purposes such as criticism or review, provided that quotations relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose.

At first sight, the scope of the citation limitation seems to be favourable to news aggregators. At domestic level, however, solutions provided for the citation exception vary. Two patterns can be distinguished: (1) quotations limitations that are not restricted to

7 Copiepresse SCRL v. Google Inc., no. 06/10.928/C, The Court of First Instance in Brussels, 13 February 2007, No. 2007/AR/1730, The Court of Appeal of Brussels, 5 May 2011.

specific purposes (Germany) or which refer to informatory purposes in general (France and Luxembourg), and (2) quotations limitations that are restricted to specific purposes such as criticism, review, research, teaching and alike (Belgium and Poland) or when making press summaries is expressly permitted either under a specific limitation (Portugal) or as quotations (Spain and the Netherlands). Some of the jurisdictions require that quotation is made in works constituting an independent whole (so no quotations *per se*) and that it should be somehow analyzed in it[8].

This suggests that news aggregators can have a problem with fulfilling quotation requirements –although it can be argued that results showed on Google News page constitute a new work, being an independent whole, it will be hard to prove that what is taken (quoted) from newspapers is then analyzed in Google News. Also, it seems that it would be easier for news aggregator to fall within quotation exception in countries where this limitation makes express reference to informatory purposes in general, such as France. Indeed, in the *Microfor* case[9] French *Cour de Cassation* concluded that indexation for information purposes does not require any authorization from the copyright owner of the referenced work since it is a short quotation allowed by the law (and the quoted parts do not need to be analyzed or commented in a new work) –as long as it does not substitute for the original work. However, this ruling was strongly criticized, on the grounds that the concept of work 'of informatory nature' is very imprecise, which seems to be a sufficient obstacle for any news aggregator to rely on the citation limitation in order to justify its activity. But even in jurisdictions where the quotation exception is not limited to any specific purpose, such as Germany, the situation is not more favourable for news aggregators. In 2010 the Federal Supreme Court in *Vorschaubilder* case[10] stated that the quotation exception, as envisaged in article 51 of the *Urheberrechtsgesetz*, does not cover displaying of thumbnails of images by the Google search engine since it lacks the legitimate purpose of quotation (meaning to elaborate on the quoted work), and because the quotation requires that there is an internal connection between the work used (or parts of it) and a new work. So the German court basically required news aggregators in Germany to fulfill similar conditions as it is in countries with citation exception restricted to specific purposes, in order to be allowed to rely on this limitation.

In the *Copiepresse* case Google invoked the citation exception so the court assessed whether Google News activity could be covered by article 21 § 1 of the Belgian Copyright Act. According to this article, a citation must aim at certain specific purpose (criticism,

8 Xalabarder R. (2012) *Google News and Copyright*, in: Lopez-Tarruella A. (ed.) *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, The Hague, The Netherlands, 138.

9 Microfor v. Le Monde, Cour de Cassation, Ass. Plén., 30 October 1987: JCP G 1988, II, 20932.

10 Vorschaubilder, BGH I ZR 69/08, 29 April 2010.

polemic, education or review) or be made in scientific works, and it must respect fair practices of the profession and be justified by the pursued goal. Google was of the opinion that exception of citation should apply to its service because it was a press review activity. The court stated that in order to rely on this exception press articles would have to be quoted in the frame of coherent comments and serve as illustrations of a review encompassing also other elements while Google News consisted of mere random juxtaposition of article fragments. The court stressed that citations should be used to illustrate or defend an opinion and concluded that Google News could not be considered as a press review. In its opinion a press review would imply a 'methodical analysis of a group elements' and 'a comparative overview of various press articles on the same topic'. The goal of a review is not to just collect elements to give a general overview on a topic but to comment upon some works. The court noticed that Google News activity consisted only of selecting and classifying articles from different sources but Google did not offer any analysis of the articles or draw any comparison between them. Neither did it express criticism or comment concerning these articles. Therefore, Google News could not benefit from the exception of quotation.

The same result was reached by the High Court of England and Wales in *Meltwater*[11] when analyzing whether this service falls within the quotation exception as envisaged in Section 30(1) CDPA. The court adopted a narrow interpretation of this provision and found a lack of critical analysis necessary to partake in criticism or review. The court focused on the most narrow use by readers, that of searching, rather than a broader possibility that readers may access articles for the purpose of criticism. Neither Meltwater's method of 'scraping' the information, nor the reader's intention in viewing the parts of the 'scraped' articles was seen to be for the purpose of criticizing or reviewing that work. *No one is criticising the parts of the article which Meltwater has 'scraped'. Nor is any one reviewing those parts of the article. Nor, generally, do they seek to criticise or review the article from which the parts are taken*[12].

3. EXCEPTION FOR REPORT ON NEWS EVENTS

Article 10bis(1) of the Berne Convention states that it shall be a matter for legislation in the countries of the Union to permit the reproduction by the press, the broad-

11 Newspaper Licensing Agency Ltd and Others v. Meltwater Holding BV and Others [2010] EWHC 3099 (Ch), [2011] EWCA Civ 890. Public Relations Consultants Association Limited (Appellant) v. The Newspaper Licensing Agency Limited and others (Respondents), [2013] UKSC 18. Meltwater, being another case considering claims against news aggregator, differs from the Infopaq (C-5/08) and Copiepresse decisions because its questions focus on whether it is the reader (end user), rather than the aggregator, that infringes.

12 Newspaper Licensing Agency Ltd and Others v. Meltwater Holding BV and Others [2011] EWCA Civ 890, 37.

casting or the communication to the public by wire of articles published in newspapers or periodicals on current economic, political or religious topics, and of broadcast works of the same character, in cases in which the reproduction, broadcasting or such communication thereof is not expressly reserved. Nevertheless, the source must always be clearly indicated; the legal consequences of a breach of this obligation shall be determined by the legislation of the country where protection is claimed. It seems, at first sight, that it is quite easy for news aggregators to rely on this exception, especially that –as against quotation limitation– it is enough to clearly mention only the source and not the name of the author. However, following closer examination of Article 10bis(1), some doubts emerge. First of all, this exception is not mandatory for Berne Union countries (although most of them introduced it). Secondly, and more importantly, the exception only applies if a copyright holder has not expressly reserved it. Thirdly, and even more importantly, articles published in newspapers or periodicals to be used under the limitation must be 'on current economic, political or religious topics'. This means that non-current topics do not fall within the exception, as well as it does not cover topics on other subjects which are often aggregated.

In the EU law, Article 5(3)(c) of the Infosoc Directive states that Member States may provide for exceptions or limitations to the rights of copyright holders in case of reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible. This provision seem to be more favourable to news aggregators since, unlike Article 10bis(1) of the Berne Convention, the EU limitation encompasses all kind of works and other subject-matter. However, it requires the reproduction of news articles be done 'by the press' and news aggregators will rather hardly qualify as 'press'[13].

This was exactly the case in *Copiepresse*. The court referred to the article 22 § 1 of the Belgian Copyright Act that states that once a work has been lawfully published, its author may not prohibit reproduction and communication to the public, for the purposes of information, of short fragments of works or of works of fine art as a whole in connection with reports on current events. The court said that this exception, as the exception of quotation, applies only when copyrighted works are accessory to the news report and are not the very object of it. Moreover, it stressed that the justification for this exception was the necessity to enable media to react quickly to events and to comment

13 Xalabarder R. (2012), 145.

upon them by using some copyrighted material even it is not possible to obtain prior permission of the copyright holder given the urgency to disseminate the information. In court's opinion Google's activity was contrary to this –Google News did not comment upon the news and, as it extracted systematically and automatically articles from the press websites, it was possible to contact the press publishers and ask for their permission. Given this, Google could not rely on the exception for report on news events in this case.

Similarly, the *Meltwater* court stated that Meltwater's users were not using the work for reporting current events for purposes of section 30(2) CDPA because Meltwater's service was available only to paid subscribers, whereas the defence provided by section 30(2) is clearly intended to protect the role of the media in informing the public about matters of current concern to the public. *Meltwater News* is not intended for public consumption; it is tailored, and addressed exclusively, to particular end users for their clients' purposes[14].

4. NEWS AGGREGATORS AND FREEDOM OF EXPRESSION

In *Copiepresse* Google not only argued that it fit into relevant exceptions for citation and news reporting, but also launched a freedom of speech argument under Article 10 of the ECHR to justify the operation of Google News service. Google claimed that while the right to freedom of expression can be limited in order to protect the rights of others, including where copyright applies, it was neither appropriate nor proportionate to do so in that case. However, the Court held that Google News does not fall within the scope of the right to freely disseminate information. In Court's opinion the fundamental right of access to information as described in Article 10 of the ECHR is not an excuse for not complying with copyright law. The court stated that the freedom of expression may not hinder the protection of the originality showed by an author in the way he expresses his ideas and concepts. It further made the point that copyright law is grounded on the balance between acknowledgment of the author's legitimate interests, on one hand, and the interests of the public and the society, on the other. In that sense freedom of expression was taken into account by the law maker when the latter provided for exceptions to copyright, such as the quotation exception[15].

The question of whether the freedom of expression right impacts protection afforded to owners of copyright was discussed in the UK's *Ashdown v Telegraph Group Ltd.*

14 Newspaper Licensing Agency Ltd and Others v. Meltwater Holding BV and Others [2011] EWCA Civ 890, 38.

15 Copiepresse SCRL v. Google Inc., No. 2007/AR/1730, The Court of Appeal of Brussels, 5 May 2011, 41-43.

case[16]. The court's conclusion was that Article 10 considerations might require to grant a public interest defence beyond the protection offered under copyright. The court assessed that copyright is essentially not a positive but a negative right, in the sense that it gives the owner of the copyright the right to prevent others from doing that which any copyright act recognises the owner alone has a right to do. Thus copyright is antithetical to freedom of expression. It prevents all, save the owner of the copyright, from expressing information in the form of the literary work protected by the copyright. *Copyright does not normally prevent the publication of the information conveyed by the literary work, in a form of words of citizen's choice. It is stretching the concept of freedom of expression to postulate that it extends to the freedom to convey ideas and information using the form of words devised by someone else. Nonetheless there are circumstances where this freedom is important and will 'trump' copyright, giving a public interest defence to a copyright infringement claim*[17].

The circumstances in which freedom of expression will prevail over copyright are rare. The public interest which newspapers serve in disclosing information can normally be protected without the newspaper copying the exact words. Occasionally, however, it is necessary for a newspaper to publish documents verbatim, for example to ensure credibility. The form of the document, on such occasions, is of equal importance to the content. The court decided that in the *Ashdown* case it would be sufficient for the *Sunday Telegraph* to publish only one or two short extracts to establish authenticity. Instead, the *Sunday Telegraph* had gone further than this: *the minute was deliberately filleted in order to extract colourful passages that were most likely to add flavour to the article and thus to appeal to the readership of the newspaper*[18]. This was furthering the Telegraph Group's commercial interests in a manner which was 'essentially journalistic'.

But it follows clearly that after the *Ashdown* case in situations where the publication of longer extracts is genuinely necessary in the public interest, newspapers could be able to rely on their right of freedom of expression. The problem with news aggregators, however, is that these services have slightly different goal than newspapers itself and so they hardly fall within the exceptions for reporting on news events.

Additionally, Google claimed that its Google News service was paralyzed by copyright, contrary to rights granted to it by the freedom of expression as envisaged in the Article 10 of ECHR. The *Copiepresse* court disagreed and stated that copyright did not prevent it from providing its service at all, as Google was free to conclude general contracts with collective management companies, which would release it from having to

16 Ashdown v Telegraph Group Ltd., [2001] EWCA Civ 1142; [2001] 4 All ER 666; [2001] 3 WLR 1368.

17 Ashdown v Telegraph Group Ltd., cit., 31.

18 Ashdown v Telegraph Group Ltd., cit., 82.

seek the prior permission from individual publishers and ensure that the latter and the authors receive the reasonable remuneration they are entitled to.

5. *FAIR USE* DEFENCE

The doctrine of fair use, as applied in common law jurisdictions, permits limited use of copyrighted material without acquiring permission from the rights holders. However, differently from the exceptions and limitations in continental jurisdictions, fair use serves only as a defence against copyright infringement and does not provide a possibility to remunerate the copyright holder. In the US the Copyright Act of 1976 sets forth four nonexclusive factors for courts to consider when determining whether a use qualifies as a fair use (17 U.S.C. § 107): (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. All these factors must be taken into account together in light of the particular circumstances of the case in order to determine whether the use is fair or not.

Of all defences to copyright infringement fair use is the most flexible. It permits courts to 'avoid rigid application of the copyright statute when it would stifle the very creativity which that law is designed to foster'[19]. At the same time, however, a fair use analysis are always very difficult for courts as they have to balance interest of copyright holders and public policy considerations. The doctrine was even called 'the most troublesome in the whole law of copyright'[20]. The best example of fair use's complicacy is the case of Google Book Library Project[21]. In this litigation between the Authors Guild and Google pending before the US Second Circuit Court of Appeals the decisions over fair use doctrine have astonished the public, to say the least. In May 2012 Judge Denny Chin let the Authors Guild sue Google on behalf of all authors whose books were scanned without permission, although Google was arguing that the Google Library Project is fair use[22]. In July 2012 the Second Circuit delivered its decision, substantially agreeing with Google and holding Judge Chin's class certification as 'premature in the absence of

19 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994).

20 Dellar v. Samuel Goldwyn, Inc., 104 F.2d 661, 662 (2nd Cir. 1939).

21 http://www.google.com/googlebooks/library/index.html.

22 The Authors Guild et al. v. Google Inc., United States District Court Sothern District of New York, Opinion 05 Civ. 8136 (DC) 10 Civ. 2977 (DC) dated 31 May 2012, available at: http://thepublicindex.org/docs/cases/authorsguild/2012-05-31-opinion.pdf, last accessed 1 May 2014.

a determination by the District Court of the merits of Google's 'fair use' defense'[23]. The Second Circuit decided to remand the cause to the District Court for consideration of the fair use issues. On 14 November 2013 Judge Chin accepted Google's argument that that its scanning of more than 20 million books for an electronic database, and making 'snippets' of text available for online searches, constituted fair use, provided that *Google Books provide significant public benefits*[24].

In light of the foregoing, the question arises whether Google News service's benefits to public policy are significant enough to justify this activity under fair use doctrine. As regards the first factor, the purpose and character of the use, a court's analysis is two-fold: first, it must evaluate the commercial nature of the use, and second, it must determine whether and to what extent the new work is transformative. A work is transformative when the new work does not 'merely supersede the objects of the original creation' but rather 'adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message'. Conversely, if the new work supersedes the use of the original, the use is likely not a fair use[25]. Additionally, courts have found transformative works that provide a social benefit or improve access to information[26]. It is even suggested that if a work is not found transformative, the analysis should end right then and there, as this factor is 'the soul of fair use'. Finally, courts have found that the more transformative a work, the less important its commercial nature[27]. In *Kelly v. Arriba Soft Corp.*[28], that focused on the use by a search engine of thumbnails of photographs, the court ruled that this use was a fair use rather than replacing the original work, since it improved access to the claimants' photographs and thus benefited to the public. Such use was deemed transformative. Similarly in *Perfect 10, Inc. v. Amazon.com, Inc.*[29] the court stated that Google's display of thumbnails was 'highly transformative' and that Google search engine was providing a significant public benefit by incorporating the preexisting works into a new one (an electronic reference tool).

---

23 Available at: http://james.grimmelmann.net/files/legal/authors-guild-appeal/opinion.pdf, last accessed 1 May 2014.

24 The Authors Guild Inc., and Betty Miles Joseph Goulden, and Jim Bouton, on behalf of themselves and all others similarly situated v. Google Inc., United States District Court Sothern District of New York, Opinion 05.
Civ. 8136 (DC) dated 14 November 2013, available at: http://pl.scribd.com/doc/184172215/Summary-judgment-order-in-Authors-Guild-v-Google-Google-Books, last accessed 1 May 2014.

25 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 583 (1994).

26 Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d, 701, 721 (9th Cir. 2007).

27 Reynolds R.F. (2010-2011) Google News and public policy's influence on fair use in online infringement controversies, Journal of Civil Rights & Economic Development 25(4), 984.

28 Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).

29 Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d, 701, 720 (9th Cir. 2007).

In considering the second factor, the nature of the copyrighted work, what matters to the courts is whether the work is creative or not, whether it has been published or not, and whether the work is still commercially available. Under a third factor, the amount and substantiality of the use, a court must explore whether the use of the copied material is reasonable compared to the original work, 'reasonable compared' understood in a way that only what is necessary to satisfy the specific purpose is taken. As general rule, the smaller the portion used, the more likely it is to be fair[30]. The fourth factor, the effect of the use upon the potential market for the work, aims at protecting the commercial market of the work and it involves the opportunities for sale or license of the work itself and its derivative works, the number of recipients, the character (commercial or non-for profit) of the institution using the work, and whether the use substitutes for the purchase of a copy of a work[31].

In the light of all above-mentioned factors, it seems to that it is not possible to clearly determine, for once and for all, whether news aggregators could be deemed as a fair use. Yet, what should be taken into account in assessing this issue is, first of all, the commercial or non-commercial character of the use. A news aggregator which include advertising is less likely to be deemed fair than the one without advertising. Then, the smaller excerpt of copyrighted work is used, the more likely a news aggregator is to be fair.

In the case of Google News, at first sight, taking into account the Google company's highly commercial nature, it seems that no compelling reasons exist to adopt the protection of the service under the fair use doctrine. However, in light of the *Kelly v. Arriba* and *Perfect 10* cases, as well as the very recent decision of Judge D. Chin in *Google Book Library Project*, it can be claimed that the US court would rule in favour of Google, finding the Google News service of transformative nature. It is because Google News may have a different purpose than print media as it meets the public's demand for more information, more quickly, whenever it wants, and offers users the power to decide what stories are most important to them. Hence, it may be asserted that Google News' transformative value overshadows its commercial nature.

On the other hand, however, it must be underlined that in some cases Google News does appear to supersede the original source of the news content as a result of its aggregation. This suggests that maybe the answer of the US court would not be so straightforward then. And that solutions maybe should be searched somewhere else.

In particular, it can be considered whether news aggregators could seek an authorization of their activities under implied license concept. This actually has been one of the mostly repeated arguments of Google that continues to highlight that it follows widely publicized and known Internet standards as to allow third party websites to 'opt out' of

30 Xalabarder (2012), 152.

31 Xalabarder (2012), 153.

its services, Google News included. Accordingly, Google argued in the *AFP* case that as AFP subscribers, licensees and AFP itself had not employed 'opt out' tools or other standard files or protocols to preclude Google News from searching and indexing the content on websites allegedly including AFP copyrighted works, they thereby allowed Google News to create links to such sites. Thus, when website operators placed content, including AFP news stories, on their websites not requiring any password or otherwise restricting access, they were intentionally making that content available to be viewed by any of the millions of users with a computer and Internet connection. Similarly, in *Copiepresse* Google insisted that press publishers had, at least implicitly, consented to the indexation by search engines. However, the *Copiepresse* court disagreed and stated that standard copyright rules provided for the necessity to obtain a prior consent from copyright holders and that they did not have to take positive measures to prevent infringements. The appeal court added that Google wrongfully deduced that since it had the technical means to browse all the publishers' sites, it meant copyright holders had given Google the permission to reproduce their works. In court's opinion no implied license derives from the mere fact that copyright owners have not implemented the technological measures that could have excluded indexation and caching by Google. On the contrary, copyright is about authors' explicit, unequivocal and prior permission, which is non-existent in the case in question[32].

6. LET'S MAKE GOOGLE PAY – THE THIRD (BETTER) WAY?

Interestingly enough, after the court door was broken down, a new practice regarding Google News appeared: in Germany, France and Belgium leading newspaper publishers had called on their governments to adopt a law to force internet search engines like Google to pay for displaying their content on services such as Google News.

The issue at stake is, in fact, whether news aggregators, failed to be allowed to rely on any of the copyright exceptions, should have to pay content providers to host its content. This contributes highly to the overall discussion on the condition of online news industry nowadays. At the moment it seems to that possible solutions are twofold. The first possibility might be that big players who run aggregation services, such as Google, enter into negotiations with local newspaper publishers in order to reach an agreement governing the use of snippets of newspaper articles by news aggregators. Another solution would be to adapt a bill that would require payment of a fee for displaying links to and snippets of articles, with the goal of recouping some of the revenues traditional news publishers have lost to the web.

32 Copiepresse SCRL v. Google Inc., No. 2007/AR/1730, The Court of Appeal of Brussels, 5 May 2011, 37.

Both models has been tried so far in different jurisdictions in Europe. In Belgium[33] and France[34] the agreements between interested parties have been concluded, although following different patterns. In Germany a bill has been introduced that extended press publishers' copyright by providing them with an ancillary right over news contents (in force as of 1st of August 2013)[35]. Passing a similar piece of legislation is being considered at the moment in Italy and Spain.

The new publisher's right in German law has been put into effect as a neighbouring right and is governed by the newly created Chapter 7 (Articles 87f-87h) of the *Urheberrechtsgesetz*. Article 87f introduces an exclusive, transferable right for a producer of a press publication (press publisher) to make the press publication or parts of it available to the public for commercial purposes, unless the parts concerned are merely individual words or smallest excerpts (snippets). If the press publication has been produced by a corporate entity, the owner of such legal entity is deemed the owner of the right. The new right expires one year after the first publication of the press publication.

The newly introduced right is tailored practically to search engine operators only, and even more visibly to the Google News service, and it has raised many critical con-

33 An agreement concluded on 12 December 2012 between Google and Belgian French-language newspaper publishers ended a six year-long running litigation between Google and Copiepresse. The agreement said that Google and Belgian French-language publishers would partner on a broad range of business initiatives. The agreement is opt-in – Belgian newspapers can decide whether to re-join Google News. Financial details of the settlement weren't disclosed. Although Google said that it is not paying the newspapers to appear on its news service, the Huffington Post reported that Google has accepted to pay a sum comprised between 2-3% (around €5 000 000) of the total turnover of Belgian French-language newspapers. Partnering with Belgian news publishers, Google Europe Blog, 12 December 2012, available at: http://googlepolicyeurope.blogspot.it/2012/12/partnering-with-belgian-news-publishers.html; Schechner S., Google Settles with Belgian Newspapers, The Wall Street Journal, 13 December 2012, available at: http://online.wsj.com/news/articles/SB10001424127887323981504578177323295632586, last accessed 1 May 2014.

34 The agreement between Google and French Government was achieved on 1 February 2013. According to its terms, Google promised to help French news organizations increase their online advertising revenue by giving them access to advertising platforms on the Internet search leader and using Google advertising technology at a reduced cost. Additionally, Google agreed to set up a 60 million euro fund to finance digital publishing innovation. The Digital Publishing Innovation Fund is aimed at helping the transformation to digital publishing by supporting work on new projects to help publishers go digital. Google clarified that the agreement means it does not have to pay for snippets of news content that appear on a Google search page – the compromise allows Google to avoid paying an ongoing licensing fee. Google and France reach landmark agreement, France24, 2 February 2013, available at: http://www.france24.com/en/20130201-google-france-reach-landmark-agreement, last accessed 1 May 2014.

35 Leistungsschutzrecht für Presseverlege (LSR).

cerns. Most of them are of a robust, constitutional nature. Apart from the rudimentary concern of prohibition of law making for individual cases, the new publishers' right creates doubts as to whether it is not in conflict with a range of fundamental rights, such as the right of search operators to the free exercise of their profession, the right to freely impart and communicate information, and the personality rights of journalists. It also poses a question of which policy rationale, other than a broad moralistic attempt to allow publishers some monetary participation from the advertising income made by search engine operators, should underpin that right[36].

Equally, the right raises concerns with regard to the overall copyright system, and in particular with regard to the copyright subject matter of it. What was described by many as a draconian 'Lex Google' was softened just one week before voting in Bundestag as lawmakers in Germany reached a compromise to water-down the language of a proposed law. Under this compromise Google (and other search engines and monitoring media firms) would still be permitted to use freely single words or short-text snippets of content from publishers' web sites in its search results. It would however require a license for use of any content beyond snippet length. This means that the German Parliament finally passed a much weaker version of the bill than first proposed. However, what the bill does not stipulate, is the precise definition of the length permitted. So maybe Google and other news aggregators have one reason less to fear the future but on the other hand uncertainty over what a snippet is, can easily result again in litigation before the courts.

It appears that new German right for press publishers looks rather to be aimed at safeguarding established (outdated) models than promoting new services and business models. What is a remarkable sign of it, is a story that happened in Germany after the new law has been introduced. Namely, in June 2013 Google announced the changes to the way Google News works in Germany[37]. According to the new rules, as of 1 August 2013 German publishers can or have to opt in to their product being indexed by Google News. This is the other way round as the previous system was based on assuming that if the material was on the Internet and not protected by 'robots.txt', then it would be included. In all other countries, however, Google has maintained in force the previous policy: if a publisher makes its content available on the net, it is included in Google News. If publishers do not wish to be included in Google News, they can use a variety of technical options (robots.txt, meta tags) use to prevent indexing by Google – or simply tell Google that their content will not be recorded.

---

36 Westkamp G. (2013) The new German publisher's right – a violation of European Law? A comment, Queen Mary Journal of Intellectual Property 3 (No. 3), 241.

37 Worstall T., Google News Goes Opt In In Germany, Forbes, 22 June 2013, available at: http://www.forbes.com/sites/timworstall/2013/06/22/google-news-goes-opt-in-in-germany/, last accessed 1 May 2014.

However, as many rightly guessed, a lot of German publishers have opted in, indeed, in order to be featured in Google News. The loss of traffic from not being in the Google News index seems to be sufficient scare for them[38]. This seems to tell a lot about the relationship between lobbying, law and the market.

7. CONCLUSIONS

The discussion about news aggregators comes at an important moment, in the midst of the debate on how best the newspaper industry should adopt to the new digital age. Currently there is good bit of legal uncertainty surrounding news aggregation activities. A body of case law addressing the ability of websites to aggregate news articles is emerging, though clear guidance for various types of news aggregators is still wanted. Several basic questions (not necessarily easy) still need to be answered to assess whether news aggregation is lawful or not, and –hence– whether and how to make their operation legal.

In particular, there is no single answer to the question whether news aggregators displaying titles, headlines, and snippets of newspapers articles are infringing copyright law. At the moment, news aggregators do not benefit from any specific statutory limitation. At the same time, they can hardly fit into existing exceptions and limitations such as exception for citation or exception in favour of communication media. What some court decisions (such as *Copiepresse* and *Megakini*[39]) show is that the statutory limitations existing in most national laws are insufficient to adjust to a rapidly evolving technological landscape, and that any exhaustive list of limitations is doomed to fail. Additionally, rather narrow interpretation of existing limitations by the courts risks making them ineffective and impossible to apply to new technologies.

Fair use / fair dealing doctrines seem to grant news aggregators more chance of succeeding but they are highly fact specific and depend very much on the circumstances of the concrete case. In addition, the non-compensated nature of fair use makes it hardly difficult to conclude that a news aggregator could be regarded a fair practice.

---

38 Lardinois F., Google Makes Google News In Germany Opt-In Only To Avoid Paying Fees Under New Copyright Law, TechCrunch, 21 June 2013, available at: http://techcrunch.com/2013/06/21/google-makes-google-news-in-germany-opt-in-only-to-avoid-paying-fees-under-new-copyright-law/, last accessed 1 May 2014.

39 Pedragosa v. Google Spain, S.L., WESTLAW AC 2008/1773. In this case the owner of the website www.megakini.es sued Google for copyright infringement by means of unauthorized displaying (and thus reproducing and/or making available) by Google its contents through Google's search engine. The court decided that Google's reproduction of the webpages html codes and contents was in order for the search engine to operate and was exempted under the temporary copies limitation.

Finally, implied license doctrines are also imperfect, as it is hard to accept the idea that newspapers publishers do not use any techniques to prevent their sites from being crawled by the so-called 'googleboots' just because they want their content to be displayed without any compensation on Google News site. This, as pointed out correctly by the *Copiepresse* court, contradicts clearly with the very idea of copyright which is about authors' explicit, unequivocal and prior permission[40]. So implied license may be eventually held true in case of general search engines but not in case news aggregation sites.

Lacking clear, harmonized rules courts sometimes try to challenge the existent situation in order to decide about the copyright infringement by news aggregators on the basis of substantiality / *de minimis* test as regards copying of copyrighted works. It means that some of the courts are likely to find that no copyright infringement results from making a list of links to news articles as this does not imply a *substantial* taking from the original webpage and, moreover, is of a temporary, incidental and minimal character, thus lacking infringing nature. However, this reasoning is likely to fail when a news aggregator provides not only links but also significant fragments of news works (so conveying essential information). Accordingly, the *Copiepresse* court seemed to suggest that Google News site could avoid liability for copyright infringement by merely reproducing titles and headlines, or –even better– merely linking titles and headlines from original websites, but not snippets of articles.

In light of all this, it is submitted that copyright law –failed to keep up with technological and social change– should be revised and adopted to current digital reality. Although the debate on how best copyright laws should answer to news aggregators' activities seems to be far from its end, the underlying idea of the discussion is that those who profit from the distribution of contents must also contribute economically to their creation. Indeed, if we look closer on the cases involving news aggregators we will see that what matters is not so much the copyright infringement but rather the conveyance of the information contained in the copyrighted works, and recovery of the investment made in its production[41].

At the moment, the possible models for regulating news aggregators activities in Europe appear to be the German (Italian? Spanish?) legislative approach and the conclusion of private agreements between interested parties. Although Google's spokespersons were very enthusiastic about the agreements in Belgium and France, saying that 'these agreements show that through business and technology partnerships we can help stimulate digital innovation for the benefit of consumers, our partners and the wider web', it

40 This actually invokes a simple comparison: if I leave my car open, with keys inside, do I say 'I want to have it stolen'? If newspapers put some content online, without using 'robots.txt' do they say 'we want to have the articles stolen (taken) by Google'?

41 Xalabarder R. (2012), 165.

does not seem the proper path to follow. As the European Publishers Council (EPC) pointed out the type of deal arranged between Google and a group of publishers does not address the continuing problem of unauthorised reuse and monetisation of content, and so does not provide the online press with the financial certainty or mechanisms for legal redress which it needs to build sustainable business models and ensure its continued investment in high-quality content'.

Rather, what is needed in longer term are solutions based on the law. Whether it can be done by means of attentively balanced statutory limitations (including remunerated compulsory licensing) or left for voluntary licensing, has to be carefully considered, and not only from the copyright but also competition law standpoint. However, in drafting any solution it must be remembered that legislation may turn out to be disadvantageous for users and the web. If snippets and headlines require licence fees, the ability to locate, and –consequently– to find, information may be curtailed as search engines could (and likely will) simply remove the publishers from their index –an approach that Google has already taken in Belgium. If this happens, locating the news becomes more difficult. Imposition of licence fees in this context may also reduce competition by making it more difficult for new entrants who cannot pay such fees, and unintentionally favouring well-funded players who can pay.

Anyway, one thing is certain –failing to provide any solution, we may risk survival of news aggregation, an activity that although some its features are criticized– provides value-added service that satisfy fundamental need in the information society. It was even suggested that by leaving the problem of news aggregators unresolved (or left to a 'theoretical voluntary licensing') we may be giving up some of the richest potentials of the Internet in exchange for a 'pyrrhic victory' for newspapers[42] and the maintenance of the copyright *status quo* (which has always been evolving with technology and markets)[43].

Technological development is always conflicting with, or at least poses difficult questions, to the existing legal *status quo.* However, technological changes may be seen not only as a threats but also challenges and opportunities to create new business models. Google News for sure is challenging nowadays.

Battles over Google News are expression of the ongoing deadlock between nations seeking to control cyberspace within their national borders and huge Internet companies like Google that want to standardize the rules of digital engagement globally. As Jan Malinowski, a media expert at the Council of Europe, says trying to get Google to pay for articles 'is like trying to ban Gutenberg's printing press in order to protect the

42 Turner M, Callaghan D. (2008) You can look but don't touch! The impact of the Google v. Copiepresse decision on the future of the Internet, European Intellectual Property Review 1, 34.

43 Xalabarder (2012), 165.

scribes'. One thing is certain about news aggregation sites: newspapers can't live with them and can't live without them.

8. BIBLIOGRAPHY

Allgrove B., Ganley P. (2007) *Search engines, data aggregators and UK copyright law: a proposal*, European Intellectual Property Review 29(6), 227-237.

Bunz M., *Rupert Murdoch: 'There's no such thing as a free news story'*, The Guardian, 1 December 2009, available at: http://www.theguardian.com/media/2009/dec/01/rupert-murdoch-no-free-news, last accessed 1 May 2014.

Hargreaves I. (2011) *Digital Opportunity. A review of Intellectual Property and Growth*, available at: http://www.ipo.gov.uk/ipreview-finalreport.pdf , last accessed 1 May 2014.

Isbell K. (2010) *The Rise of the News Aggregator: Legal Implications and Best Practices*. Available at: http://cyber.law.harvard.edu/publications, last accessed 1 May 2014.

Kreutzer T. (2011) *German copyright policy 2011: Introduction of a new neighbouring right for press publishers?*, Computer Law & Security Review (CLSR), 27, 214-216.

Lardinois F., *Google Makes Google News In Germany Opt-In Only To Avoid Paying Fees Under New Copyright Law*, TechCrunch, 21 June 2013, available at: http://techcrunch.com/2013/06/21/google-makes-google-news-in-germany-opt-in-only-to-avoid-paying-fees-under-new-copyright-law/, last accessed 1 May 2014.

Lopez-Tarruella A. (2012) *Introduction: Google Pushing the Boundaries of Law*, in: Lopez-Tarruella A. (ed.) *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, The Hague, The Netherlands.

Lopez-Tarruella A. (ed.) (2012) *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, The Hague, The Netherlands.

McCarthy C., *Agence France-Presse, Google settle copyright dispute*, CNET News, 6 April 2007, available at: http://news.cnet.com/2100-1030_3-6174008.html?part=rss&tag=2547-1_3-0-20&subj=news, last accessed 1 May 2014.

McCarthy C., *Google Reveals payment deal with AP*, CNET News, 3 August 2006, available at: http://news.cnet.com/Google-reveals-payment-deal-with-AP/2100-1030_3-6102109.html, last accessed 1 May 2014.

Partnering with Belgian news publishers, Google Europe Blog, 12 December 2012, available at: http://googlepolicyeurope.blogspot.it/2012/12/partnering-with-belgian-news-publishers.html, last accessed 1 May 2014.

Peguera M., *Website operator sentenced to 18 months of prison for linking to P2P*, ISP Liability. Spanish Case Law & More, 17 November 2013, available at: https://ispliability.wordpress.com/2013/11/17/website-operator-sentenced-to-18-months-of-prison-for-linking-to-p2p/, last accessed 1 May 2014.

Reynolds R.F. (2010-2011) *Google News and public policy's influence on fair use in online infringement controversies*, Journal of Civil Rights & Economic Development 25(4), 973-997.

Rosati E. (2013) *The German 'Google Tax' law: groovy or greedy?*, Journal of Intellectual Property Law & Practice 8 (No. 7), 497.

Stanganelli M. (2012) *Spreading the news online: a fine balance of copyright and freedom of expression in news aggregation*, European Intellectual Property Review 34 (11), 745-753.

Turner M, Callaghan D. (2008) *You can look but don't touch! The impact of the Google v. Copiepresse decision on the future of the Internet*, European Intellectual Property Review 1, 34-38.

Westkamp G. (2013) *The new German publisher's right – a violation of European Law? A comment*, Queen Mary Journal of Intellectual Property 3 (No. 3), 241-250.

Worstall T., *Google News Goes Opt In In Germany*, Forbes, 22 June 2013, available at: http://www.forbes.com/sites/timworstall/2013/06/22/google-news-goes-opt-in-in-germany/, last accessed 1 May 2014.

Xalabarder R. (2012) *Google News and Copyright*, in: Lopez-Tarruella A. (ed.) *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, The Hague, The Netherlands.

7

LEGAL CHALLENGES FOR ONLINE DIGITAL LIBRARIES

Argyri Panezi
Ph.D. Candidate,
European University Institute, Department of Law

ABSTRACT: Libraries have traditionally played a central role in collecting, organizing material and giving wide access to culture and knowledge. Does the existing copyright framework provide enough space for online digital libraries to claim an equivalent central role in the online space? This article explores the legal challenges for online digital libraries' collection building. The materials that build the content of a library fall broadly under three categories with respect to their copyright status: copyrighted works, works with ambivalent copyright status (such as orphan and out-of-print works) and public domain works. In the paper, I try to answer a number of legal questions related to these three categories of works, inter alia licensing and e-lending as well as digital exhaustion, and also defend the value of creating and sustaining robust digital libraries online. The paper will conclude on how the theory of the commons can improve the existing legal framework and strengthen the libraries' position in order to sustain valuable knowledge commons supporting the ever-growing network ecosystem. Thus, I emphasize the value of maintaining a growing public domain that can be organized and digitally accessible online.

KEYWORDS: digitization, EU digital policy, digital libraries, licensing and e-lending, digital exhaustion, orphan works, public domain, knowledge commons.

1. INTRODUCTION: WHY IS THE DISCUSSION ABOUT DIGITIZATION POLICY AND THE CREATION OF DIGITAL LIBRARIES IMPORTANT

Why do policy makers care about digital libraries, whose purpose is mainly public, at a time when the e-book market is evolving exactly as a market, without public purpose considerations?[1] There are important reasons why we still need to care about libraries also in the digital age. Libraries have traditionally played a central role in collecting, organizing material and giving wide access to culture and knowledge. While a market is consumer-preference driven, culture and knowledge (scientific or academic etc.) needs

1 E-book readers, the need for interoperability, price-fixing, competition and dominance (see Amazon) are among the biggest issues debated today as regards the new and quickly developing e-book market *See* Angela Daly, E-book monopolies and the law, 18 Media and Arts Law Review, 350 *et. seq.*

to be organized and preserved at times beyond markets. This is obviously the case, for example, with niche scholarship on topics as specific as medieval medical history. Thus, a task of assembling human knowledge online extends beyond the digitization of popular literature titles. All the more, the intellectual works, after being assembled, need to be curated, organized and presented in a useful way to the public. These are all tasks that libraries are traditionally committed to. Therefore, the question that this article wishes to explore further is on this very issue of the role of the digital libraries. **Do existing regulatory frameworks, mainly copyright limitations and exceptions, provide enough space for online digital libraries to claim an equivalent central role in the online space?**

In broad terms, the two jurisdictions that I take into account are the American and the European. Digitization has been a clear priority in the EU digital agenda for some time now.[2] At the same time the issue has been and continues to be heavily debated in the US in the context of the Google Books litigation and with more digital libraries initiatives having started in parallel.[3]

This article begins by mapping the relevant legal issues involved. I first explore the legal challenges for online digital libraries' collection building with regard to copyrighted works, works with ambivalent copyright status (such as orphan and out-of-print works) and public domain works. Second, I look at what is the additional value of a digital library, which should make policy makers differentiate them and perhaps entrust them with the special role of offering wide access to intellectual works and preferential treatment in the form of copyright limitations and exceptions.

2. LEGAL CHALLENGES FOR ONLINE DIGITAL LIBRARIES' COLLECTION-BUILDING

The materials that build the content of a library fall under three categories with respect to their copyright status: copyrighted works, orphan works and out-of-print works. These three I categorize together as works with ambivalent or, rather, problema-

2 The legal bases thus far are mostly soft law provisions: Commission and Council recommendations and conclusions (article 292 TFEU), press releases and reports (such as the Comité des Sages report) and some specific legislation initiated (notably the Orphan Works Directive). Most importantly, though, the ongoing copyright reform consultation (public consultation on the review of the EU copyright rules) can potentially play a big role further producing hard law changes with direct effects on digitization and the creation of libraries online.
For the EU's digital libraries initiative see http://ec.europa.eu/information_society/activities/digital_libraries/index_en.htm.

3 *See* primarily the Digital Public Library of America (DPLA). For the ongoing efforts of the US Copyright Office – and also the legislator looks to legislate, for example on the issue of orphan works *see* http://www.copyright.gov/orphan/ (inquiry ongoing).

tic copyright status (such as orphan and out-of-print works) and public domain works. A complete digital library should be able to offer access to all of these types of works.

I explore the collection that builds a digital library following this categorization since the legal status then dictates accessibility. A copyrighted book cannot be offered online without the right-holders' permission, and is accessible under their terms.

I will examine these three categories consecutively. I begin with copyrighted works. Besides being a very big corpus of works, it is also a hugely important one given that most recent books and intellectual works in general are usually under copyright. Even if some copyrighted works are freely accessibly, for example under a certain type of Creative Commons license, they are still as such under the copyright framework –essentially meaning that they are not part of the public domain, unless the right-holders have explicitly given up their rights.

Starting with the copyrighted works, the questions that emerge broadly occur in two phases, one during the *input* phase, how does the library get access to the copyrighted material, and the second during the *output* phase, in what manner is the library allowed to offer access to the public, its users. I will look at the distribution right that copyright affords to right-holders and also exhaustion and the big debate of digital exhaustion.

Then I explore the orphan works puzzle and the issue of out-of-print works, and propose a policy solution or change that strengthens the case for digital libraries: entrusting the orphans and the out-of-print works to the public domain. Last, I examine the public domain works and whether the legislator (the copyright policy maker) indeed promotes access and reuse of this category of materials. I conclude arguing how could digital libraries be the institutional gatekeepers of these bodies of works managed primarily (where possible) as commons.

3. COPYRIGHTED WORKS

3.1. Distribution right and exhaustion

Two central economic rights that copyright affords to right-holders are, first and foremost, the reproduction right (right to make copies) and, second, the right to distribution (right to distribute copies).[4] The right to distribute copies is relevant to the discussion of library lending and, by consequence, to e-lending as well (following subchapter).

Article 6 of the WIPO Copyright Treaty is devoted to the *Right of Distribution* and states that:

4 Paul Goldstein and Bernt Hugenholtz, International Copyright, Principles, Law and Practice, Oxford (3rd ed.), pp. 307-321.

> 1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing the ***making available to the public*** of the original and copies of their works through sale or other transfer of ownership.
>
> (2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the ***exhaustion*** of the right in paragraph (1) applies ***after the first sale*** or other transfer of ownership of the original or a copy of the work with the authorization of the author.
>
> (emphasis added)

As demonstrated in the wording of the above Article 6 in paragraph 2, the distribution right is limited by exhaustion («principle of exhaustion» or «first sale» doctrine). Once copies of works have been placed in the market with the right holder's consent, further re-distribution (for example, resale) does not need to be authorized. This is a long-standing rule in the EU jurisdictions where the principle of exhaustion has been established by the European Court of Justice and codified in the Information Society Directive of 2001 article 4(2). In addition, there is a territorial effect within the entire EU jurisdiction as first sale of a work in one EU member state will exhaust the distribution right of the author also in all other member states. In US law the US Copyright Act recognizes the same rule in section 109(a).

Traditionally, once a library purchases a book from a publisher, the exhaustion or first-sale doctrine releases the copy from further copyright control.[5] Library lending of printed books finds its legal basis exactly on this doctrine. This is not the case today for e-books and e-lending. According to the Agreed Statements concerning the WIPO Copyright Treaty (statements concerning Articles 6 and 7), the expressions «copies» and «original and copies», subject to the right of distribution and the right of rental under the said Articles, refer exclusively to ***fixed copies*** that can be put into circulation as ***tangible objects***.[6]

Thus, currently copyright law worldwide explicitly only grants exhaustion to tangible objects, such as printed books.[7] The situation for digital works, including e-books, is unclear. According to Harald Müller, from a legal point of view libraries cannot lend e-books out because there is no statutory legal instrument available for e-book loan services by libraries.[8] I am not entirely certain that this conclusion holds unconditionally. This author, however, suggests that since the current regulatory framework does not protect libraries, as exhaustion does for printed books, they must lobby to create new legal instruments enabling e-lending.

---

5 *Ibid*, p. 316. There is however a «Public Lending Right» in the European Union jurisdictions, as per the E.C. Rental Right Directive.

6 *See* http://www.wipo.int/meetings/en/html.jsp?file=/redocs/mdocs/diplconf/en/crnr_dc/crnr_dc_96.html.

7 Harald Müller, Legal aspects of e-books and interlibrary loan, Interlending & Document Supply 40/3 (2012) 150-155, available at http://www.emeraldinsight.com/journals.htm?articleid=17047187, p. 152.

8 *Ibid*.

3.2. Licensing and e-lending

Given the lack of clear regulatory framework covering e-lending, libraries that wish to make e-books available for lending to their users, are currently facing several licensing practices and models offered by publishers or right holders. This is the case both for purely digital libraries and for traditional libraries whishing to offer digital services on top of their 'traditional' services. The framework is still quite unclear for a number of reasons, both practical and legal. E-lending is a rather new service, which they can now offer only once they negotiate with publishers and clear licensing terms. This is quite different than what libraries are used to in terms of lending services for print books. To lend print books all libraries do, traditionally, is acquiring copies, which are then part of their own collection. In the legal sense the exhaustion or first sale doctrine, as we will analyze further, has been covering the lending of print books. The situation with e-books, however, is different. Access to e-books takes place on the basis of licenses rather than purchase.

From the publishers' side, the business models for licensing are still new as they experiment with different levels of access as well as with pricing. The e-book market is rapidly expanding[9] and, as the market is expanding, publishers experiment with several digital publishing business models. David O'Brien, Urs Gasser and John Palfrey classify the models used by e-book distributors to libraries in three general categories (a distributor is usually the intermediate that sells to the libraries access to e-books, often from multiple publishers[10/11]): 1. the perpetual access model, 2. the subscription model and 3.

---

9 Notably in 2011 Amazon.com officially announced that it sells more kindle books than print books. Amazon press release: http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1565581&highlight.
See also http://www.nytimes.com/2011/05/20/technology/20amazon.html.
In 2012 Amazon.co.uk made the same announcement. *See* http://www.theguardian.com/books/2012/aug/06/amazon-kindle-ebook-sales-overtake-print.
At the same time, not all publishers permit e-book lending in libraries. Some see libraries as competitors in the digital distribution of books and, do not offer library e-lending programs. Among big publishers that allow e-book lending are Random House, Penguin, Hachette and HarperCollins, (David O'Brien, Urs Gasser, John Palfrey, supra note 15, p. 9). Notably Simon & Schuster did not license any e-books and only in April announced a one year pilot program with New York libraries, *see* http://www.forbes.com/sites/davidvinjamuri/2013/04/15/simon-schuster-tests-ebook-lending-with-new-york-libraries/.

10 David O'Brien, Urs Gasser, John Palfrey, E-Books in Libraries: A Briefing Document Developed in Preparation for a Workshop on E-Lending in Libraries, Berkman Center Research Publication No. 2012-15, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2111396##, page 8.

11 The most commonly used distributors from the US libraries are OverDrive, NetLibrary, Gale/Cengage and EBSCOhost. *Ibid* (O'Brien, Gasser &Palfrey), also citing Library Journal E-book Survey in «Ebooks the New Normal: Ebook Penetration & Use in US Public Libraries», Library Journal, 2011, p.24, available at http://www.thedigitalshift.com/research/.

the pay-per-view model.[12]

The ***perpetual access*** model allows libraries to integrate e-books to their collection through an e-book collection management software platform, usually hosted not by the library itself but by an e-book vendor.[13] Access is determined by the terms of each license. The DRM technology used by the vendor platform limits how can the file be accessed and shared.[14] This model usually tries to replicate print books lending in that it limits access to the e-book in time (loan periods are usually between 14 and 21 days), and allows one (or some) patron at a time. The costs for this model include platform maintenance fees and also generally e-book titles are more expensive compared to purchase of the print book.[15]

The ***subscription*** model gives the libraries the option of subscribing to a database of e-book titles for a pre-determined period of time.[16] Upon termination of the subscription the library no longer has access to the database unless it renews its subscription. The advantage of this model is that an unlimited number of patrons can access the same e-book simultaneously. However, the cost per user for the library is quite high. Another disadvantage is that vendors avoid offering «front list» titles (publisher's list of new titles) with this model.[17]

In the ***pay-per-view*** model, used less frequently than the other two, libraries pay a certain fee in order to display a list of available titles to their users.[18] With every use of each title, however, the library needs to pay an additional fee per copy. The flat fee for accessing the e-book list is much lower compared to the subscription model but then the renting fee per copy rises.

There is also a ***patron-driven acquisition*** model, which resembles the pay-per-view model. If a pre-determined number of patrons request a certain book title, the library will acquire a copy from the distributor.[19] The difference here is that libraries actually acquire ownership of the titles unlike with the pay-per-view model.

Upon first examination, these models have a number of advantages and disadvantages. Access to «front-list» titles is one common problem. Balancing the costs of the model

12 O'Brien, Gasser & Palfrey, supra note 10, p. 10.

13 *Ibid*, p. 14.

14 *Ibid*.

15 *Ibid*, p. 15.

16 *Ibid*, p. 17.

17 *Ibid*.

18 *Ibid*, p. 19.

19 *Ibid*, p. 11. As the authors explain, this model is very useful for libraries offering bestselling e-books that are in high-demand.

with the patrons' usage (demand) is probably the most difficult issue. The most problematic aspect is that so long as these models offer licensing rights and not ownership to the libraries, access is always subject to the libraries' ability to pay fees (which are a form of subscription fees). Without clear ownership, the libraries' abilities to build, maintain and curate a collection is substantially discounted. The advantage of these models is their flexibility. Publishers, intermediaries and libraries can collaborate to adjust packages to needs and to user's demands. This is at least true in theory, bearing also in mind, however, the negotiating power of each party. Copyright holders might be nervous that the ease of use of a digital library will mean that consumers will stop buying books (cannibalization of sales). While physical books degrade, thus the second hand markets are less of a threat to the first hand markets; it is true that digital books don't degrade. Thus, the negotiation and contracting process for in-copyright works between libraries and active right holders is not simple, as the latter will be looking for revenue streams and perhaps the maximum possible profit.[20] All the more is the case with their collective societies.

3.3. Legal constructions proposed to address the problem

In view of the above described situation, scholarship looks at copyright theory (and beyond it) to discover the solutions to legal obstacles that libraries are currently facing with e-lending and also formulate arguments on how to apply the exhaustion or first-sale doctrine also to digital works.

a) Legislative amendment of copyright law/ special library exemption

Legislative history of the US first-sale doctrine legislation shows that library lending is one of the underlying reasons for the existence of the doctrine.[21] A similar rationale can be traced in the various EU jurisdictions and the copyright exceptions they provide for libraries.[22] Yet, given the lack of legislative provisions that address the same issue for digital works and the lack of any explicit legislative exemption for libraries giving as regards e-lending, some scholars argue that there is a need for new legislative action. The United States Copyright Office had reached an analogous conclusion in a policy document in 2011.[23] According to the Copyright Office, section 108 of 17

20 Randal C. Picker, « After Google Book Search: Rebooting the Digital Library» (John M. Olin Program in Law and Economics Working Paper No. 559, 2011), p. 9.

21 Matthew Chiarizio, An American tragedy: e-books, licenses, and the end of public lending libraries?, 66 Vand. L. Rev. 615, at p. 620.

22 Goldstein & Hugenholtz, supra note 4, p. 316.

23 US Copyright Office, Legal issues in Mass Digitization: a preliminary analysis and discussion document, Office of the register of copyrights, Oct. 2011, available at http://www.copyright.gov/docs/massdigitization/USCOMassDigitization_October2011.pdf, pp. 19-22.

U.S.C. enacted in 1987 «was shaped by the technology and concerns of the pre-digital age.»[24] The appropriate scope of library exceptions might, thus, need to be revisited in a coherent and systematic manner.

During the summer of 2013 the Dutch association of public libraries (Vereniging van Openbare Bibliotheken (VOB)) initiated a test case in their national court of first instance about the right to lend e-books in public libraries.[25] The libraries assert that e-lending is (or should be) included in the copyright exception for libraries and ask for a preliminary reference to be sent to the European Court of Justice. The Minister of Education, Culture and Science, on the basis of a special report prepared by the IVIR Institute (Institute for Information Law at the University of Amsterdam), already denied such right.[26] The report observed that e-lending already occurs in public libraries in several jurisdictions and is not based on copyright limitations or exceptions, but proceeds on the basis of contractual agreements. The central question that the report posed was «whether e-lending by public libraries is covered by the existing public lending right regime of the Dutch Copyright Act (*Auteurswet*), and whether the European copyright framework leaves enough space for a copyright limitation or exception at the national level.» [27] Both questions were answered negatively.

The recent Dutch report on online e-book lending through libraries[28] adds that the Copyright Directive of 2001 provides for an *exhaustive* list of permitted limitations and exceptions to copyright, including several exceptions that concern public libraries. It stresses that the existing European copyright framework, in its current state, does not leave room for the introduction at the national level of a (compensated or non-compensated) copyright exception permitting online lending of e-books by public libraries.[29]

As we noted above, one can conclude that libraries need to lobby for a statutory solution for their e-book activities. [30] For that reason they need to lobby in order to secure that the privileges they enjoy as institutions in the analogue world need to be enjoyed also in the digital world. Indeed, libraries already do that. The International Federation

24 *Ibid*, p. 20.

25 See http://www.futureofcopyright.com/home/blog-post/2013/06/18/dutch-public-libraries-are-commencing-a-test-case-on-e-lending.html.

26 The report entitled «Online uitlenen van e-books door bibliotheken» (= Online Lending of e-books through libraries) is available in Dutch at: http://www.ivir.nl/publicaties/poort/Online_uitlenen_van_e-books.pdf and includes a summary in English.

27 *Ibid*.

28 The Dutch report, supra note 26.

29 *Ibid*, English summary.

30 Müller, supra note 7, p. 154.

of Library Associations (IFLA) for example has taken the lead with a concrete treaty proposal on limitations and exceptions for libraries and archives.[31]

b) Courts' intervention to uphold digital exhaustion

Other scholars are more skeptical about the possibility and practicability of a legislative solution.[32] Nevertheless, as copyright law has strong roots in judicial construction, with most doctrines originating in common law case-law, these scholars trust that the courts can effectively manage the new challenges that the digital era poses to libraries. These would include e-lending.

Aaron Perzanowski and Jason Schultz observe that with the shift towards digital markets the first sale doctrine is increasingly marginalized.[33] They suggest that courts should remedy that, since a legislative change towards this end is difficult or unlikely to occur today. In their article on digital exhaustion the authors argue that the common law judge (they are writing in the setting of the US jurisdiction) can apply a broader principle of copyright exhaustion to which first sale is part. This broader principle, as emerges from several cases, guarantees a set of privileges for the user, namely alienation, renewal, repair, adaptation and preservation.[34]

Judges are called to apply the exhaustion principle to digital copies as they already do to computer programs (17 USC section 117). According to Perzanowski and Schultz courts are already empowered to do so.[35] It is important that the benefits of the first sale doctrine are also enjoyed for digital works (as «functionally equivalent privileges»[36]). The reasons for this are traced in the ***benefits of the first sale doctrine or exhaustion*** in general. These benefits are:

i. ***increased access***: availability as well as affordability of copyrighted works is increased. After the first sale, the right holder lawfully looses control over the copies. Second hand bookstores, libraries, video rental shops and auctions sites are then able to operate as a secondary market which accelerates access and pushes prices down so that they are affordable to audiences that would otherwise not be consumers in the primary market.[37]

31 *See* http://www.ifla.org/node/5856.

32 Aaron Perzanowski and Jason Schultz, Digital Exhaustion, 58 UCLA Law Review (2011) 889-946.

33 *Ibid*, pp. 892 *et seq*.

34 *Ibid*, p. 912 and pp. 913-922 citing ample case-law where the rights to repair and renewal, rights to adaptation and modification, and display and performance rights are established.

35 *Ibid*, p. 936.

36 *Ibid*, p. 937.

37 *Ibid*, p. 894-5. The authors cite evidence that secondary markets are better at price discrimination and at maximizing social welfare than copyright owners.

ii. ***preservation***: specifically for works that are no longer commercially interesting, as for example out-of-print books or orphan works, the first sale doctrine assists in maintaining circulation and thus preserving and keeping cultural products alive.[38]

iii. ***privacy***: consumer's privacy and anonymity are threatened when right holders preserve control over the circulation of their work after the first sale has occurred.[39] Reader's privacy is an important issue when it comes to e-lending and the question is who controls the data that reveal reading habits of users; libraries or private distributors that operate DRM platforms?

iv. ***transactional clarity***: transaction costs are rendered disproportionately high and cost inefficient, when relatively low-cost copyrighted works require complex limitations and control over redistribution after the first sale.[40]

v. ***user innovation***: there is effective incentive for right holders to innovate in order to compete with secondary markets. This way, new or better creations such as updated works or additional content are promoted.[41]

vi. ***platform competition***: consumer lock-in is reduced with regards to platforms, when consumers are allowed to alienate their digital purchases from the platforms and transfer them when switching platforms without the need to repurchase.[42] The argument promotes interoperability; that is, for example, the ability to read the same e-book on a kindle or an i-pad.

3.4. Allowing a young market to mature through competition or intervening when contracts appear to override copyright law?

Matthew Chiarizio notably suggests that the best course of action for the government is to not intervene but allow the stakeholders «a chance to find a solution within the existing legal framework».[43] This suggestion emphasizes the still undeveloped nature of the relevant market, with a lot of potential to experiment and innovate in viable e-lending models.

See also Anthony Reese, The first sale doctrine in the era of digital networks, 44 B. C. L. Rev. 577. Reese emphasizes *affordability* and *availability* as key benefits (pp. 644-652).

38 *Ibid*, p. 895.

39 *Ibid*, p. 896. See also Julie E. Cohen, A right to read anonymously: a closer look at «Copyright management» in Cyberspace, 28 Conn. L. Rev. 981 (1996).

40 *Ibid*, p 896.

41 *Ibid*, p. 897.

42 *Ibid*, pp. 900-901.

43 Chiarizio, supra note 21, p. 641.

The idea that any intervention would be either premature or disrupt the growth of the market does not fully address an important factor: the asymmetries in the involved parties' bargaining powers. Libraries have traditionally enjoyed privileges for a number of (valid) reasons. The challenges they face in the digital era are numerous. In a digital world where electronic retailers have started offering services such as 'Amazon's Kindle Owner's Lending Library',[44] trusting the negotiating power of libraries and letting them survive the e-book market as created without any equivalent to the digital exhaustion doctrine might be too optimistic.

On the other hand, investigating the current business models for licensing that enable library e-lending, one cannot help but conclude that this is another case where contracts are claiming to supersede copyright law. The relation between the legislative exceptions and limitations to copyright and freedom of contract to restrict such exceptions and limitations in a private contract has been a difficult issue that courts as well as scholars faced already before the e-lending discussion.[45] More specifically, courts have already faced the issue of boundaries between ownership and licensing in several contexts. There is, for example, ample case-law around computer software attempting to determine whether a transaction was a license or a sale.[46]

The problem with e-lending is that the major publishers, contractually superior to small libraries or generally libraries with serious budget limitations, are now establishing contractual conditions that exceed the monopoly afforded by copyright.[47] Without the limitations that the exhaustion or first sale doctrine place on the copyright monopoly of the right holders, distribution of digital works circumvents the rationale behind copyright (to guarantee enough, but not more than that, incentives for creation) and promotes rent-seeking practices.

---

44 *See* http://www.amazon.com/gp/feature.html?docId=1000739811.
See also Bill Rosenblatt, A nail in public libraries coffins, available at http://copyrightandtechnology.com/2012/05/20/a-nail-in-public-libraries-coffins/.
In view of Amazon's launching of a lending library, Lloyd Jassin interestingly finds that the next great e-book debate will be on how to define subscription revenue. *See* Lloyd Jassin, Amazon's lending library liability, available at http://www.copylaw.org/2011/11/amazons-lending-library-liability.html.

45 *See* Orit Fischman Afori, The battle over public e-libraries – tacking stock and moving ahead, IIC (2013) 44: 392-417, at p 401.

46 From US case-law see: Vernor v. Autodesk Inc.,621 F.3d 1102, 1110-11 (9th Cir. 2010) MDY Industries. v. Blizzard Entertainment, Inc., 629 F. 3d 928, 938 (9th Cir. 2010) Apple, Inc. v. Psyster Corp., 658 F.3d 1150, 1155-56 (9th Cir. 2011) UMG Recordings, Inc. v. Augusto, 628 F.3d 1175, 1180 (9th Cir. 2011).

47 Fischman Afori, supra note 45, p. 393.

Copyright law claims the ability to maintain the delicate balance between different interests. The various exceptions and limitations are also attempting to maintain the same balance. When contracts afford to right holders' benefits that far exceed the rights afforded by copyright law this already delicate balance is distorted. This seems to be the case with licensing models that publishers currently offer to libraries. Academic libraries are particularly suffering from this development. Restrictive licenses then threat to become a real obstacle to research and teaching.[48] This also explains the spread of the open access movement and the role that major libraries seek to play leading the policy debate and demanding that electronic subscriptions must be rethought.[49]

In all, the sticking contradiction to the right holders' legal rights regarding a print book renders the need for clarity in the regulatory framework for e-lending pressing. The increased cost for online versions of works is a burden that we cannot just assume that libraries will simply adapt to. As Reese explains, a decline in affordability and of access via libraries is a crucial problem.[50] Under the current framework he identifies a possibility that either digital works will be available by libraries at greater cost or, even worse, many works will not be available in libraries at all.[51] If we value the role of the library and wish to preserve it in the digital era as well, the situation is alerting and calls for regulatory action.

4. ORPHAN AND OUT-OF-PRINT WORKS

4.1. The Orphans' Puzzle

Fay Kanin, Chair of the Library of Congress National Film Preservation Board (NFPB), coined the term 'orphan works' to inclusively describe *works protected under copyright whose copyright holder cannot be identified or located*.

According to one account, there are two approaches in definitions to the orphan works problem.[52] The first focuses on the inability of a potential user to identify and locate the right-holder from whom permission is to be sought. The other approach places the inability of the user to easily obtain permission to use a particular work central to

48 *Ibid*, p. 404.

49 *See* open letter from Harvard University Library: «Faculty Advisory Council Memorandum on Journal Pricing», April 17, 2012, available at http://isites.harvard.edu/icb/icb.do?keyword=k77982&tabgroupid=icb.tabgroup143448.

50 Reese, supra note 37, p.646.

51 *Ibid*.

52 David Hansen, Orphan Works: Definitional Issues, Berkley Digital Library Copyright Project White Paper #1, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1974614.

the problem (broader approach, also argued by Google during the Google Books controversy). Out-of-print books, for example, are a category, which includes orphan works, without the two categories overlapping. This broader issue of the inability or difficulty to connect to the copyright owners has led to the perception of orphan works as a greater problem of market failure.[53] A potential user faces disproportionate transaction costs to obtain authorization from a right-holder, as well as the risk of infringement liability. Thus, he will usually forgo the use «*even though had the user been able to locate the copyright owner, a deal would have been struck for that use*.»[54] Although it is to be expected that rights-clearance involves certain transaction costs, with orphan works these costs become disproportionally high and results are still not guaranteed.

According to librarians, there is a great amount of orphan works for which it is estimated that even after extensive research, no further information can be found. However, knowing the exact size of the problem is important in order to be able to calculate the social and economic costs and benefits of possible solutions to the problem.[55] The very nature of orphan works renders the finding of both firm quantitative and qualitative data a difficult task. This also explains why the size of the problem has not been calculated in a consistent manner.[56]

The root of the orphan works problem, which renders the quest for a solution from the EU and the US so difficult, is found primarily in the expansions that copyright law

53 *Ibid*, p.1.

54 Lydia Pallas Loren, Abandoning the Orphans: An Open Access Approach to Hostage Works, 27 Berkeley Tech L. J. (2012 forthcoming), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2049685, p. 3.

55 *See* also the JISC 2009 report, analyzing data from an online survey of over 500 organizations suggesting that many public sector organizations in the UK are themselves unsure of the extend of the problem. The report is available at http://www.jisc.ac.uk/media/documents/publications/infromthecoldv1.pdf.

56 For example, the British Library has estimated that 40 % of its in-copyright collections are orphan: Report of the 'Comité des Sages' reflection group pm bringing Europe's cultural heritage online, The New Renaissance, available at http://ec.europa.eu/culture/pdf/report_Comite_des_Sages.pdf, p. 16.
David Drummond, Google's general counsel estimated that relatively few, under 20%, of the books in the Google Books corpus will ultimately turn out to be orphan (also relying on his positive predictions for Google's project incentivizing copyright owners to come forward). See, Pamela Samuelson, Google Book Search and the future of Books in Cyberspace, 94 Minn. L. Rev. 1308 (2009-2010), p. 1323 citing to the Competition and Commerce in Digital Books hearing before the House of Representatives, available at http://judiciary.house.gov/hearings/hear_090910.html. At the same time for the same project Jonathan Band estimated that around 75% of out-of-print books will remain unclaimed: *See* Jonathan Band, The long and winding road to the Google Books Settlement, 8 J.Marshall Rev. Intell. Prop. L. 227, (2009), p. 294.

saw in the past few decades; extensions of copyright duration along with elimination of registration, renewal and notice requirement for copyright protection (these results are also due to the Berne Convention rules). As simply explained by Olive Huang, longer copyright terms create longer periods over which copyright owners can change hands and become even more difficult to trace.[57]

In any event, orphan works constitute an appreciable corpus of works that need to be taken into account in any discussion about a digital library. As the Google Books and Hathitrust litigations showed, orphans are also a far from negligible stake for stakeholders.

4.2. Legislative attempts and responses thus far

Starting with the premise that the owner (author or subsequent right-holder) is absent, there is indeed an interesting question that lingers with respect to orphan works: Why has it thus far proven so difficult to introduce reform in a property law area where owners of works are absent (thus by definition are unable themselves to lobby), while users of works lobby for reform?[58]

---

57 Olive Huang, U.S. Copyright Office Orphan Works in 21 Berkley Tech. L. J. 265 (2006), p. 268. *See* also David Hansen, Orphan Works: Causes of the problem, Berkley Digital Library Copyright Project White Paper #3, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038068. According to Hansen the orphan works problem may have existed in theory since first copyright laws came into effect, if one defines the problem broadly as the situation where the owner of a copyrighted work cannot be located and asked for authorization by someone who wants to use it.
In her recent article Lydia Pallas Loren argues that the problem can also be traced back to terminology. Indeed, the orphan metaphor is misleading. Loren claims that the use of the metaphor is now also causing difficulties to address the problem. She proposes the term «hostage» works instead. Lydia Pallas Loren, supra note 54. For the notion of the «romantic author» *see* Mark A. Lemley, Romantic authorship and the rhetoric of property, 75 Tex. L. Rev. 873 (1997).

58 *See* Ariel Katz, The Orphans, the Market, and the Copyright Dogma: a modest solution for a grand problem, 27 Berkeley Technology Law Journal 1285, pp. 1322-1331 at p. 1337, where he remarkably notes: *A discussion of solutions to the orphan works problem will not be complete before addressing why has it been so challenging to find an acceptable and workable solution to this problem in the first place. The difficulty is puzzling because owners of orphan works are, by definition, absent from the debate about orphan works, and normally, when discussions about contemplated reforms do not involve those who might be directly affected by them, one could expect that reform would be easy. Specifically,* ***one could expect that in a setting where users lobby for reform that would allow them to use orphan works, and owners of those works are absent, passing a pro-user reform (even overly pro-user) would be a breeze.*** *Therefore, the fact that it has been difficult to find an acceptable solution, and that many of the proposed solutions involve serious impediments on using orphan works, suggest that the political economy of the orphan works problem is complicated, and that there is much*

Indeed, in the US there have been two unsuccessful attempts to legislate the orphan works problem: first, with the Orphan Works Act of 2006.[59] Later two other bills were introduced, i.e., the Orphan Works Act of 2008[60], and the Shawn Bentley Orphan Works Act of 2008.[61] There is already one report on orphan works prepared by the United States Copyright Office and published in January 2006. Indicating that there will be indeed another attempt to legislate, the United States Copyright Office recently issued a broad notice of inquiry in the Federal Register, seeking comments from the public regarding the current state of play for orphan works.[62]

In the EU there have been concrete policy developments with the Orphan Works Directive, 2012/28/EU, adopted the previous October.[63] This directive 'on certain permitted uses of orphan works' sets out common rules for the digitization and online display of orphan works.[64] The directive applies only to works that are first published (broadcasted or made publicly available by the beneficiaries) in the territory of an EU Member State. In all, the solutions that the Directive provides are quite narrow in scope since they apply to a particular class of users and uses and only to particular types of works. One could question, whether there is any plausible reason to discriminate between public interest institutions and others (private/ for profit bodies). Some questions arise also with regard to the (con-

at stake –not necessarily for the interests of orphan owners, but for the interests of those who speak on their behalf.

59 H.R. 5439, 109th Congress, 2nd session, 22 May 2006.

60 H.R. 5889, 110th Congress, 2nd session, 24 April 2008.

61 S. 2913, 110th Congress, 2nd session, 24 April 2008.

62 *See* at http://www.copyright.gov/orphan/. Collective societies seem to be taking the lead against orphan works legislation, while the academic world together with libraries (comments from librarians, associations of libraries and University libraries) are recognizing a real problem that needs comprehensive solution.

63 Available at http://ec.europa.eu/internal_market/copyright/orphan_works/index_en.htm.

64 Directive preamble, point 3. The Directive is complementing and without prejudice to the existing 20 September 2011 Memorandum of Understanding on key principles on the digitization and making available of out-of-commerce works: Memo available at http://europa.eu/rapid/press-release_MEMO-11-619_en.htm. In order to establish whether a work is orphan the above mentioned institutions shall carry out a 'diligent search' according to the requirements of article 3 of the directive, keeping records of their searches on a publicly accessible online database. What constitutes a 'diligent search' is outlined in more detail in a Memorandum of Understanding on diligent search guidelines for orphan works. Once designated as orphan, it may be used (digitized and made available) by the institutions *only in order to achieve aims related to their public-interest missions, in particular the preservation of, the restoration of, and the provision of cultural and educational access to works and phonograms contained in their collection* (art. 6(2) of the Directive). The directive provides for a system of compensation if the right holder(s) is found at a later stage (article 5 of the Directive).

siderable) discretion of member States with respect to the implementation of the directive. Given that the EU directive is narrow and leaves ample room for different interpretations, and that the member States have now started the debate at a national level, it is reasonable to conclude that even after the passing of the directive, the debate around orphan works is far from closed also in the jurisdictions of the EU.

All the more, what is important for us here is that the directive is not adequately addressing the big issue of mass digitization. The diligent search requirement it sets (Orphan Works Directive, article 3) is neither very clear nor efficient to enable mass rights clearance for orphans. This is, however, the most important issue for the creation of digital libraries, at least as regards this body of works. Thus, the directive cannot be easily seen as solving how can digital libraries deal with orphan works, which they have to do in a mass rather than *in concreto* or sporadic scale.

4.3. Scholarly proposed solutions

There is ample legal scholarship examining the orphan works problem. Some of this scholarship includes systematic mapping and evaluation of possible solutions to the issue.[65] [66] Thus, many solutions have been proposed including ***centrally administered licenses*** (this is the Canadian system), ***extended collective licensing*** (applied in various Scandinavian jurisdictions, a system where management of rights is assigned to a collective society, which negotiates freely on behalf of owners), ***limited liability***, meaning limiting remedies after a diligent search for right-holders (this is the solution favored by the US Copyright Office in both 2006 and 2008 attempts to legislate), ***statutory limitation or exception***, ***access and re-use systems tailored to fair use***, suggesting that fair use exceptions suffice to solve the problem of orphan works when applied correctly. In addition to the above categories of approaches, there is one more general category; ***broader policy reforms*** that seek to address copyright formalities and duration, and library, archive and museum privileges, while having the ability to mitigate or partially address the orphan works problem. The objectives here are: 1.reinvigoration of copyright formalities and reduction of the effect of increased copyright duration and 2.reforms to library, archive, and museum privileges that would allow those institutions to provide new forms of access to the works in their collection.

65 Stef van Gompel & Bernt Hugenholtz, The orphan works problem: the copyright conundrum of digitizing large scale audiovisual archives, and how to solve it, Popular Communication: The International Journal of Media and Culture, Vol. 8, No. 1, pp. 61-71, 2010, available at http://www.ivir.nl/publications/vangompel/the_orphan_works_problem.pdf.

66 David Hansen, Orphan Works: Mapping the possible solution spaces, Berkley Digital Library Copyright Project White Paper #2, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2019121.

4.4. Out-of-print works

Out-of-print or out-of-commerce works have known or traceable authors, unlike orphans. However, for systematic purposes, I include them in the same problematic as orphan works. While digitization can bring new life to these works, the efficiency argument that I will make in the following chapter works well for both, when seen as 'abandoned' property works. Unlike the orphan works issue, which became hugely debated, especially after the Google Books litigation is the US, the literature on out-of-print works is less. There has been interesting economic analyses for potential markets for out-of-print works.[67] For the purposes of this paper, however, I will deal with this issue far less extensively and grouped with the orphan works where the emphasis, also from the scholarship is based.

4.5. A solution that strengthens the case for digital libraries: entrusting the orphans and the out-of-print works to the public domain

Given both the complexity of the orphans problem and the lack of a clear and strong policy argument to maintain their copyright status, as well as the existence of out-of-print works, which have the potential of regaining a 'digital life', it is arguably much more efficient and a better policy option to entrust both to the public domain. From the perspective of the creator, the entitlement is lost` by virtue of the creator's absence or the lack of further incentives to commercialize, and because the transaction with a user, if at all possible, has become inefficient. From the perspective of the public, I argue that there should be a mere freedom in accessing and using the orphans and out-of-print works and they should be added to the corpus of the public domain. Freeing both sooner rather than later is a solution that both avoids the utility loss of 'abandoned' works and simultaneously generates great societal benefits by enlarging the public domain. Becoming part of the public domain's commons, orphans and out-of-print works are not losing the connection to a supposedly father/romantic author[68] but are gaining a family at large, the community enjoying them and benefiting from them, utilizing them and making them relevant.

While intellectual property law generally implies an overall analogy to property law, ironically this has not been the case with orphans or out-of-print works. In property law there is a number of rules and doctrines in both civil and common law jurisdictions

67 *See* for example Smith, Michael D. and Telang, Rahul and Zhang, Yi, Analysis of the Potential Market for Out-of-Print eBooks (August 4, 2012), available at http://ssrn.com/abstract=2141422.

68 A. Chander and M. Sunder, The Romance of the Public Domain, 92 California Law Review, 1331- 1373 (2004), p. 1338.

that favor the loss of property once abandoned for enough time (rules on adverse possession, rules determining the faith of abandoned property etc.). The rationale behind such doctrines is to penalize neglectful owners by granting, under certain requirements, property either to other (adverse) possessors, or to the public. At the same time they seek to give property owners the incentive to be attentive to their assets.[69] The irony is that in this case borrowing doctrines from property law would rather go against sustaining intellectual property rights on orphans.

My main argument however is that the body institutionally most capable of protecting works with unclear or dubious copyright status is neither a private company like Google, nor a collective society like Authors Guild, arguably not even the state, which can design compulsory licensing schemes. It is rather the public as a whole, the same body that has an interest collectively in using and reusing information as input to new production. As Elinor Ostrom has demonstrated, studies «challenge the presumption that governments always do a better job than users in organizing and protecting important resources».[70]

Practically, what I propose is that this body of works shall be managed as commons along with the ones already in the public domain (following chapter). Successful management of commons is not a simple task. I propose that the central role of trust between key players (contributors, users and gatekeepers) shall be played by libraries, institutions that already enjoy a stern status and can be trusted to play the crucial role of gatekeepers for common intellectual recourses. The proposal needs further elaboration, which is beyond the scope of this article. Here I merely formulate the argument that current orphans and out-of-print works offer a great opportunity for institutional innovation with respect to commons.

5. PUBLIC DOMAIN WORKS

The third category, public domain works, are rather the 'easier case' when it comes to collection building for digital libraries. They are freed from copyright and available for scanning by any stakeholder, private or public, for the purposes of digitization. Quoting Paul Heald, the legal consequence of public domain status is that all users may appropriate freely without interference from competing claimants.[71] Although there

69 *Ibid*, p. 12.

70 Elinor Ostrom, Beyond Markets and States: Polycentric Governance of Complex Economic Systems, Nobel Prize lecture, December 8, 2009, available at http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf, p. 409.

71 Paul Heald, The public domain, Richard Watt (ed.), The Law and Economics of Copyright (Routledge 2014), Forthcoming, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2362983, p.1.

are many different definitions of the public domain (mainly depending on jurisdiction) most are more or less accepting at least this consequence as fact and as the common denominator.[72]

Commission Recommendation of 27 October 2011 on the digitization and online accessibility of cultural material and digitization preservation understands online accessibility of public domain works as follows (article 5):[73] 1. It must be ensured that the material **remains** in the public domain after digitization, 2. The widest possible **access and reuse of the material for non-commercial and commercial purposes** must be promoted and 3. Measures to limit the use of intrusive watermarks or other visual protection measures that reduce usability of the digitized public domain material must be taken.

What does it mean, however, for the legislator or the policy maker to promote access and reuse of the public domain works? Before going to this question, we need to see why there is a need to promote access and reuse of the public domain in general; in other words, what is the value or the social utility of the public domain. According to Samuelson the public domain serves at least eight distinct values: it serves as 1. building blocks for the creation of new knowledge and enables 2. competitive imitation, 3. follow-on innovation, 4. low cost access to information, 5. public access to cultural heritage, 6. education, 7. public health and safety, and last but not least enables 8. deliberative democracy.[74] Paul Heald searching the same question of the value of maintaining a growing public domain draws an important conclusion: the value of the public domain will be its 'net' value, that is the value generated by the work being in the public domain over above that it would generate under copyright[75]

Going back to the issue of the legislator promoting access and re-usage of public domain works, the specific question this article focuses on is whether the existing legal framework assists or, at least, encourages libraries to provide this access and thus to promote these values or benefits generated by the public domain. I believe that the current copyright framework and general copyright policy does not promote this access and reuse in a consistent and sufficient manner. Firstly, the copyright term is excessive, currently lifetime of the author plus 70 years in both sides of the Atlantic, blocking new

72 For a consistent effort to map the public domain *see* Pamela Samuelson, Challenges in Mapping the Public Domain, in The Future of the Public Domain: Identifying the Commons in Information Law (Lucie Guibault /P. Bernt Hugenholtz (eds)), pp. 7-25.

73 *See* also Recital 13.

74 Samuelson, supra note 72, p. 22.

75 Paul Heald, The public domain, Richard Watt (ed.), The Law and Economics of Copyright (Routledge 2014), Forthcoming, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2362983, p.1, citing Pollock, Stepan, & Valimakki, Valuing the EU Public Domain, Cambridge Working Papers in Economics 1047 (2010), 1-54.

important works from entering the public domain quicker after they have generated the necessary profits to the creator. The optimal scope of copyright for protected works is debated. It has also been famously modeled by Landes and Posner who concluded that because of discounting to present value, extensions of the copyright term beyond twenty or twenty-five years have little incentive effect for creators, which is the main rationale behind copyright laws in the first place.[76] Existing formal models, however, tend to focus on the optimal term length for the recovery of sunk costs during a period of supra competitive pricing, without considering the relevance of access and distribution of existing works or the costs imposed on follow-on creation and the other said values. With an excessive copyright term, copyright policy is by definition not sided at the public domain side. Second, there is no copyright rule forbidding or dis-incentivizing the propertizing of public domain works. Thus, private companies are able to make profit out of this pool of sources offering them online as part of a service and locking them with DRM systems even though they are legally free from copyright. This is the case, for example, with Google that began to scan books taken from libraries and made also public domain books part of their business plan for the Google Books service. Google profits from advertising, and thus offers the scanned public domain books for free to the users, however it is part of a commercial service. Also there are other examples of services that make profit directly from making available public domain works.[77]

6. CONCLUSION: THE NEED OF A REGULATORY FRAMEWORK SUPPORTING ONLINE DIGITAL LIBRARIES AND SUSTAINING VALUABLE KNOWLEDGE COMMONS

The Internet's potential to revolutionize the way we access and then produce culture and knowledge should be supported by a regulatory framework that promotes wide accessibility, in order to sustain valuable commons supporting the ever-growing network ecosystem. Digital libraries are a central paradigm in this respect. Thinking about libraries, a helpful conceptualization is that of a «Zone of accessible information».[78] It is

76 Landes & Posner, The Economic Structure of Intellectual Property Law, Harvard University Press, 2003, p.70 and 210 et. seq.

77 *See* for example http://www.forgottenbooks.org/. At the same time, there are volunteer efforts of assembling and offering public domain works for free, such as the Project Gutenberg (started in 1971 by Michael Hart) which is the first important digital library project online, exactly offering works that are free from copyright (under US law). The project has now over 45,000 items in its collection. *See* http://www.gutenberg.org/ last visited May 19, 2014.

78 *See* Sherman and Wiseman, Toward an Indigenous Public Domain?, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain: Identifying the Commons in Information Law, Kluwer, 2006, p. 259 et. seq.

necessary to enlarge the corpus of these accessible materials, if we believe in the value of creating and sustaining robust access-points to knowledge online. Furthermore, within libraries, information is organized in a way meaningful to the users. As Randal Picker has noted (on the opportunity of the rejection of the Google Books Settlement in 2011) «**we are at a point of rebooting how we design our digital library future**».[79] What seems already undesirable is a digital library monopoly. What we should instead want to foster is a rich digital library **ecosystem**.[80]

James Boyle describes the evolution of the Internet from a government project to the White Paper, to a private industry.[81] The Internet has started from being an agora, then a market and now it returns to becoming an agora again.[82] This becomes more clear when we look at Jonathan Zittrain's five conceptual layers to the network; physical; protocol; applications; content; and social layer.[83] The layers represent the division of labor among people constructing and/or using the network. The past associates with proprietary networks and hierarchies, whereas the present facilitates «polyarchies». Nowadays, however, we observe a cultural shift towards alternatives to either the market's contracts-based production (employers in firms) or property-based market-value systems (individuals in the market following «signals»).[84] Other production models are mostly commons-based or peer-production models particularly visible in the digital world (for example open-source software).

In the same vein, we observe a shift from strict and expanding copyright laws to peer-production of knowledge, information and culture.[85] Simultaneously, we witness the phenomenon of «cultural agoraphobia» (openness aversion) whereby we underestimate the «importance, viability, and productive power of open systems, open networks, and nonproprietary production.»[86] This article seeks to be a basis for the **consideration of the role of the digital library in fighting against this cultural agoraphobia.** In the digital era space is virtually unlimited (information are stored in the cloud), knowledge

79 Picker, supra note 20, p. 1.

80 *Ibid*, p.2.

81 James Boyle, The Public Domain: Enclosing the Commons of the Mind (Yale University Press 2008) available at http://thepublicdomain.org/thepublicdomain1.pdf, p.85 et seq.

82 *See* http://www.nytimes.com/2009/09/13/weekinreview/13giridharadas.html.

83 Jonathan Zittrain, The Future of the Internet -- And How to Stop It (Yale University Press & Penguin UK 2008) available at http://futureoftheinternet.org/static/ZittrainTheFutureoftheInternet.pdf p.67.

84 Yochai Benkler, Coase's Penguin, or, Linux and The Nature of the Firm, 112 Yale Law Journal 369 (2002) available at http://www.yale.edu/yalelj/112/BenklerWEB.pdf.

85 Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, (Yale University Press 2006) available at http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf, p.23.

86 Boyle, supra note 81, p.231.

is accessible and books are fireproof; libraries cannot turn to ashes like the library of Alexandria famously did. But how rich and accessible are they? How accessible can they be and how accessible should they be to the public? Indeed, the Internet's potential to revolutionize the way we access and then produce culture and knowledge should be supported by a regulatory framework sustaining online digital libraries, as public service institutions beyond markets and beyond the division of private and public.

7. BIBLIOGRAPHY

Jonathan Band, The long and winding road to the Google Books Settlement, 8 J.Marshall Rev. Intell. Prop. L. 227, (2009)

Yochai Benkler, «Coase's Penguin, or, Linux and The Nature of the Firm,» 112 Yale Law Journal 369 (2002)

Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom, (Yale University Press 2006)

James Boyle, The Public Domain: Enclosing the Commons of the Mind (Yale University Press 2008)

A. Chander and M. Sunder, The Romance of the Public Domain, 92 California Law Review, 1331- 1373 (2004)

Matthew Chiarizio, An American tragedy: e-books, licenses, and the end of public lending libraries?, 66 Vand. L. Rev. 615

Julie E. Cohen, A right to read anonymously: a closer look at «Copyright management» in Cyberspace, 28 Conn. L. Rev. 981 (1996)

Angela Daly, E-book monopolies and the law, 18 Media and Arts Law Review, 350 *et. seq*.

G. Faulhaber & D. Farber, Spectrum management: Property rights, markets and the commons, in: Proceedings of the Telecommunications Policy Research Conference, Alexandria, VA (Oct. 2003) available at http://rider.wharton.upenn.edu/~faulhabe/SPECTRUM_MANAGEMENTv51.pdf

Orit Fischman Afori, The battle over public e-libraries – tacking stock and moving ahead, IIC (2013) 44: 392-417, at p 401

Paul Goldstein and Bernt Hugenholtz, International Copyright, Principles, Law and Practice, Oxford (3rd ed.)

Stef van Gompel and Bernt Hugenholtz, The orphan works problem: the copyright conundrum of digitizing large scale audiovisual archives, and how to solve it, Popular Communication: The International Journal of Media and Culture, Vol. 8, No. 1, pp. 61-71, 2010, available at http://www.ivir.nl/publications/vangompel/the_orphan_works_problem.pdf.

David Hansen, Orphan Works: Definitional Issues, Berkley Digital Library Copyright Project White Paper #1, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1974614

David Hansen, Orphan Works: Mapping the possible solution spaces, Berkley Digital Library Copyright Project White Paper #2, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2019121

David Hansen, Orphan Works: Causes of the problem, Berkley Digital Library Copyright Project White Paper #3, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038068

Paul Heald, The public domain, Richard Watt (ed.), The Law and Economics of Copyright (Routledge 2014), Forthcoming, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2362983

Olive Huang, U.S. Copyright Office Orphan Works in 21 Berkley Tech. L. J. 265 (2006)

Ariel Katz, The Orphans, the Market, and the Copyright Dogma: a modest solution for a grand problem, 27 Berkeley Technology Law Journal 1285, pp. 1322-1331

Mark A. Lemley, Romantic authorship and the rhetoric of property, 75 Tex. L. Rev. 873 (1997)

Harald Müller, Legal aspects of e-books and interlibrary loan, Interlending & Document Supply 40/3 (2012) 150-155, available at http://www.emeraldinsight.com/journals.htm?articleid=17047187

IVIR Report entitled «Online uitlenen van e-books door bibliotheken» (= Online Lending of e-books through libraries) is available in Dutch at: http://www.ivir.nl/publicaties/poort/Online_uitlenen_van_e-books.pdf (English summary included)

David O'Brien, Urs Gasser, John Palfrey, E-Books in Libraries: A Briefing Document Developed in Preparation for a Workshop on E-Lending in Libraries, Berkman Center Research Publication No. 2012-15, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2111396##

Elinor Ostrom, Beyond Markets and States: Polycentric Governance of Complex Economic Systems, Nobel Prize lecture, December 8, 2009, available at http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf

Lydia Pallas Loren, Abandoning the Orphans: An Open Access Approach to Hostage Works, 27 Berkeley Tech L. J. (2012 forthcoming), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2049685

Aaron Perzanowski & Jason Schultz, Digital Exhaustion, 58 UCLA Law Review (2011) 889-946

Randal C. Picker, « After Google Book Search: Rebooting the Digital Library» (John M. Olin Program in Law and Economics Working Paper No. 559, 2011)

Anthony Reese, The first sale doctrine in the era of digital networks, 44 B. C. L. Rev. 577. Reese emphasizes *affordability* and *availability* as key benefits (pp. 644- 652)

Pamela Samuelson, Challenges in Mapping the Public Domain, in The Future of the Public Domain: Identifying the Commons in Information Law (Lucie Guibault /P. Bernt Hugenholtz (eds)), pp. 7-25.

Pamela Samuelson, Google Book Search and the future of Books in Cyberspace, 94 Minn. L. Rev. 1308 (2009-2010)

Eli Salzberger, Economic Analysis of the Public Domain, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain, 27-58

Smith, Michael D. and Telang, Rahul and Zhang, Yi, Analysis of the Potential Market for Out-of-Print eBooks (August 4, 2012). Available at http://ssrn.com/abstract=2141422

US Copyright Office, Legal issues in Mass Digitization: a preliminary analysis and discussion document, Office of the register of copyrights, Oct. 2011, available at http://www.copyright.gov/docs/massdigitization/USCOMassDigitization_October2011.pdf

Jonathan Zittrain, The Future of the Internet – And How to Stop It (Yale University Press & Penguin UK (2008)

8

OF E-BOOKS AND ONLINE AGENCIES: HOW CAN EU COMPETITION LAW BE APPLIED SO AS TO SAFEGUARD PLURALISM IN THE PUBLISHING INDUSTRY?

Konstantina Bania
Doctoral Researcher, Department of Law, EUI

ABSTRACT: This paper discusses the impact of the European Commission's antitrust practice on pluralism in the e-book market. More particularly, the study examines the recent E-Books Commitments Decision, which dealt with the online agency agreements concluded between online retailer Apple and six large publishing houses. In this decision, the Commission focused on the anti-competitive concerted practice (collusion) in which these undertakings were allegedly involved, but largely abstained from taking a position on where the online agency model stands in EU competition law terms. Should online agency agreements be regarded as «genuine» agency arrangements thereby escaping antitrust scrutiny altogether? If not, how could an exemption under Article 101(3) TFEU be granted to a «false» agency so as to ensure that consumers receive a fair share of the benefits resulting from the agreement? How does the characterization as «genuine» or «false» agency affect pluralism in the book markets? From a law and economics perspective, the article argues that an online agency agreement should not be condemned simply on the grounds that it does not afford the retailers the ability to offer lower prices and that, depending on market conditions, relevant arrangements may confer several, both price and quality-related, advantages upon the consumers. But, far from the Commission's simplistic approach, a careful case-by-case assessment of numerous parameters is needed in order to reach safe conclusions as to whether this system safeguards competition, pluralism and ultimately consumer interests.

KEYWORDS: e-books, digital publishing, antitrust, online agency, wholesale model, fixed book pricing, Amazon, Apple.

1. INTRODUCTION

Book publishing is not only the oldest sector of the European media and content industries, but also the most powerful. On a global scale, the book market is the only one where EU firms lead, accounting for more than a third of the total global book market revenue.[1] In addition to its significant contribution to the strengthening of Eu-

1 European Commission, Joint Research Center Technical Report on Statistical, Ecosystems and Competitiveness Analysis of the Media and Content Industries: The Publishing Industry 2012, 9,

ropean competitiveness vis-à-vis third countries, this industry plays a significant role in achieving broader societal goals, because books are products with public utility components. Literature is one of the most important means to disseminate information and knowledge (learned people imply positive external effects to their milieu) and improve communication by enhancing a population's lingual competence.[2] Furthermore, constituting one of the foundation stones of nations, books have long been acknowledged as one of the most valuable expressions of cultural heritage and, as such, a building block in European integration.[3] As a result, the book publishing sector has traditionally been perceived as a vehicle for promoting and cultural and linguistic diversity across the EU.[4]

Considering the above, it is not surprising that several Member States have enacted special rules governing the book trade, the most popular (and probably the most controversial) being fixed book pricing (hereafter FBP).[5] On the basis of this pricing model, the publisher may set the retail prices of the titles it produces and the bookseller is not permitted to offer discounts or any other forms of promotion, unless the publisher allows it. Fixed book pricing has been embraced inter alia on the grounds that it helps advance pluralism in the book market.[6] More particularly, while introducing a ban on price competition, fixed book pricing may lead to a broad range of titles, including more literary books that would not have found their way into the market under a free pricing system, and an extensive network of bookstores which, being offered the security of a stable market, may perform the role of guardians of literary creation by carrying low-demand books. On this basis, in several Member States, a favorable competition regime has been set that allows FBP arrangements to escape general antitrust prohibitions.[7] At EU level, FBP agreements enjoy no such privilege with cross-border FBP agreements falling under the general antitrust rules. However, and while the Commission has acknowledged the

available at: http://is.jrc.ec.europa.eu/pages/ISG/documents/BookReportwithcovers.pdf (Note: all websites referred to throughout the paper were re-accessed on 10/05/2014).

2 Ringstad 2010, 354.

3 See, for instance, Communication from the Commission, Books and Reading: A cultural challenge for Europe, COM(89) 258 final.

4 European Parliament Report with recommendations to the Commission on the drawing-up of a directive of the European Parliament and of the Council on the fixing of book prices (2001/2061(INI)) (Rothley Report), 11.

5 Other policy instruments include State subsidies and lower VATs. For an overview see Appelman and Canoy 2002, pp. 587 et seq.

6 See, for instance, *the Spanish* Ley 10/2007, de 22 de junio, de la lectura, del libro y de las bibliotecas Publicado en BOE núm. 150 de 23 de Junio de 2007, Preàmbulo.

7 This was the case e.g. for the UK prior to the dismantlement of the Net Book Agreement which escaped the general antitrust prohibitions as laid down in the UK Resale Prices Act and the Restrictive Practices Act. See Utton 2000, 116. This was also the case in the Netherlands, see Vedder 2003, 340.

positive effects brought about by fixed book prices,[8] it has not formulated a competition practice that would promote a pluralistic book market. Concerned about stimulating price competition, the Commission dismantled FBP agreements basing its decisions on the contestable assumption that FBP leads to higher prices. Reacting to this approach, both the European Parliament and the Council adopted non-binding acts asking the Commission to re-consider its approach to these arrangements.[9]

But, as a result of developments that followed these decisions, most notably a deregulatory approach to the sector promoted by several Member States and the subsequent dismantlement of FBP systems, the issue of agreements establishing a fixed book pricing system went dormant for about eight years when, in early 2010, the Commission opened an investigation into arrangements made between publishers and online retailer Apple (**the E-books case**[10]) that revivified the debate. These arrangements, being very similar to traditional FBP systems in that publishers would set the prices for the e-books sold on Apple's iBooks Store and Apple would not offer any discounts, reopened the long-standing discussion over where FBP stands in EU competition law terms. But, besides the controversies surrounding FBP, the particularities of the e-book markets and the business model employed to support the sales of the e-books (agency model) have created additional challenges in keeping the e-book markets competitive, innovative and pluralistic which the Commission has not lived up to. More particularly, in its decision, the Commission refrained from giving concrete answers on whether Article 101 TFEU applies to online agency agreements and if so, how pluralism-specific considerations can be taken into account in an assessment under Article 101(3) TFEU as primary EU law (e.g. Article 167(4) TFEU) dictates.

This paper discusses in detail the Commission's approach to fixed pricing in digital publishing and argues that, while agency agreements establishing an FBP system should not be regarded as a sine-qua-non condition for the preservation of pluralism in the e-book market, they should not be condemned simply on the grounds that they do not afford the booksellers the ability to offer lower prices. The article is structured as follows. The first part describes the facts of the E-Books case. The second part attempts to answer

8 See, for instance, Communication from the Commission of 3 August 1989 on 'Books and reading: A cultural challenge for Europe' (COM(1989)258).

9 See, e.g. Resolution of 12 February 2001 on the application of national fixed book-price systems, [2001] OJ C 73/03.

10 Commission decision of 12.12.2012 addressed to: - Hachette Livre SA, - HarperCollins Publishers Limited, HarperCollins Publishers, L.L.C., - Georg von Holtzbrinck GmbH & Co. KG, Verlagsgruppe Georg von Holtzbrinck GmbH, - Simon & Schuster Inc., Simon & Schuster (UK) Ltd, Simon & Schuster Digital Sales, Inc., - Apple, Inc. relating to a proceeding under Article 101 of the Treaty on the Functioning of the European Union and Article 53 of the EEA Agreement Case COMP/39847 - E-Books, C (2012) 9288 (consolidated version) (hereafter referred to as the Commitments Decision).

the questions which the E-Books case gave rise to, questions that the Commission left unanswered. The third part assesses whether the commitments that were imposed on the publishers involved in the E-Books case are indeed adequate to safeguard either price competition or pluralism in the e-book market. Finally, some conclusions are drawn.

2. THE E-BOOKS CASE: A SHORT DESCRIPTION OF THE FACTS

The E-Books case concerns the allegedly anti-competitive conduct of Apple and publishers[11] Hachette, HarperCollins, Penguin, Macmillan and Simon & Schuster (hereinafter collectively referred to as Publishers) in respect of the sale of e-books to consumers. The facts of this case can be summarized as follows: In January 2010, the Publishers signed **agency agreements** with Apple governing sales of e-books in the US. Under these agreements, **the Publishers would set the prices for e-books made available on Apple's iBooks Store whereas Apple would be remunerated by payment of a commission equal to 30% of the retail price paid by consumers**.[12] This type of contractual relationship was substantially different from the one the Publishers had established with Amazon in 2007 when, after Amazon launched its e-reader Kindle, demand for e-books significantly increased.[13] More particularly, prior to entering into agency agreements with Apple, the Publishers sold e-books to retailers mostly under the **wholesale model**. Under this model, **e-books were sold to the retailers at a wholesale price below the suggested retail price set by the publishers (wholesale prices were generally up to 50% of the e-book list price).**[14] **The key element of such agreements is that retailers are free to determine the retail prices charged to consumers.**[15] Between March and December 2010, the Publishers initiated negotiations with Apple regarding sales of e-books under the agency model in the United Kingdom, France and Germany.[16] These agreements, which were signed shortly thereafter, were very similar to the US contracts.[17]

In March 2011, the Commission announced that it had initiated inspections at the premises of firms active in the e-book market.[18] Based on these inspections, the

11 Commitments Decision, para. 1.

12 Ibid., Fn. 4, paras. 31 and 36.

13 Ibid., para. 18.

14 Ibid., paras. 19-20.

15 Ibid., para. 21.

16 Ibid., para. 40.

17 Ibid., paras. 41 et seq.

18 European Commission, Antitrust: Commission confirms unannounced inspections in the e-book publishing sector, MEMO/11/126, 02/03/2011.

Commission decided to open formal antitrust proceedings to investigate whether the publishers had, «possibly with the help of Apple, engaged in anti-competitive practices affecting the sale of e-books».[19] Throughout its inquiry, the Commission concentrated on the collusion aspects of the case. The Commission placed particular emphasis on the exchange of contacts between the Publishers which, concerned about Amazon's heavy discounts policy, reportedly came together to coordinate the pricing terms of the agreements signed with Apple. [20] According to the Commission, Apple played a major role in this effort by ensuring that each of the Publishers knew that the others were negotiating with it on the same pricing conditions.[21] This coordination gave strong indications that the Publishers and Apple ***«engaged in a concerted practice with the object of raising retail prices of e-books in the EEA or preventing the emergence of lower prices in the EEA for e-books, in breach of Article 101 of the TFEU»***.[22] In subsequent discussions with the Commission, the parties proposed undertakings which, following a market test, were considered appropriate to address the Commission's concerns and, as such, led to the adoption of a commitments decision.[23] But, before discussing this decision in more detail, it is best to start the analysis of the E-Books case from the questions that were left unanswered. After having examined the issues to which this case gave rise, we will be better placed to assess whether the commitments accepted by the Commission were indeed adequate to alleviate relevant concerns.

3. THE E-BOOKS CASE: THE QUESTIONS LEFT UNANSWERED

In the commitments decision, the Commission carefully avoided taking a position on the agency agreements concluded between Apple and the publishers ***absent the concerted practice***. While this issue was raised by market players in the context of the market test conducted by the Commission prior to its final assessment of the undertakings proposed by the involved firms, it limited itself to noting that «its concerns […] ***do not relate to the legitimate use of the agency model*** for the sale of e-books» [emphasis added].[24] In strict procedural terms, the Commission was not bound to conduct an analysis of the alignment of these agreements (or the agency model as a business strategy in general) with EU competition law. The Commission enjoys a large margin of discre-

19 European Commission, Antitrust: Commission opens formal proceedings to investigate sales of e-books, Press Release IP/11/1509.

20 Commitments decision, paras. 22-23.

21 Ibid., paras. 33-34.

22 European Commission, Final Report of the Hearing Officer [2013] OJ C 73/06, para. 4.

23 Commitments decision, para. 5.

24 Commitments decision, para. 153.

tion when defining the scope of an investigation it opens[25] and, since, following its preliminary assessment, it decided to focus on **the way** in which the Publishers had switched to agency (cartel) rather than **the content** of the agreements they had concluded with Apple, the commitments procedure essentially aimed at identifying the most adequate solution to restore the conditions of competition that existed prior to the possible concerted practice. However, in practice, the Commission has more often than not given its opinion on issues it was not required to address in its assessments in order to provide guidance to market players for developing their activities without falling foul of competition law.[26] Since the agency model is gaining popularity in the Internet economy in general and in the media industry in particular, the Commission should have grasped the opportunity to clarify a rather blurred framework in which businesses entering into an agency relationship operate. Could agency agreements between online retailers and publishers be regarded as «genuine» agency agreements thereby rendering Article 101(1) TFEU inapplicable? If not, which parameters should the Commission take into account when considering whether to grant an exemption under Article 101(3) TFEU? These are the questions I will seek to answer here, always with a view to examining how the various approaches to relevant arrangements can safeguard pluralism in the book market.

3.1. Could agency agreements between online retailers and publishers be regarded as «genuine» agency agreements?

Agency agreements «cover the situation in which a legal or physical person (the agent) is vested with the power to negotiate and/or conclude contracts on behalf of another person (the principal), either in the agent's own name or in the name of the principal, for the purchase of goods or services by the principal, or sale of goods or services by the principal».[27] Agency agreements fall short of Article 101(1) TFEU.[28] Thus, clauses restrictive of competition, including resale price maintenance, may escape Article 101(1) TFEU, if they form part of a «true» agency arrangement. Yet, and while the legal implications of establishing such a contractual relationship have long been clarified,[29] the conditions under which agency agreements are immune from EU competition law have been rather ambiguous.

---

25 Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU, 2011/C 308/06, paras. 17 et seq.

26 See, for instance, Commission Decision of 25 November 1981 relating to a proceeding under Article 85 of the EEC Treaty (IV/428 - VBBB/VBVB), 82/123/EEC, [1982] OJ L 54/36, para. 48.

27 Commission Guidelines on Vertical Restraints [2000] OJ C 291/01, para. 12. This definition is repeated verbatim in the most recent version of the Guidelines [2010] OJ C 130/01, para. 12.

28 Commission Guidelines on Vertical Restraints, [2010] OJ C 130/01, para. 18.

29 The Commission affirmed the special regime that agency agreements enjoy as early as 1962. See Notice on Exclusive Dealing Contracts with Commercial Agents, OJ 1962 139/2921.

The first (and -what seems to be in current practice- decisive) criterion relates to the allocation of commercial and financial risks; where the agent assumes no such risks, she is deemed to be a genuine agent.[30] Two appear to be the key factors to reach this conclusion. First, ownership of the contract goods should not vest in the agent and second, the agent should not bear any direct or indirect risks in respect of the contracts concluded by herself on behalf of the principal, including transport costs, advertising costs, liability vis-à-vis third parties and liability vis-à-vis the principal for non-performance by the customer.[31] Determining, however, whether this criterion is fulfilled is not a straightforward exercise. For instance, one issue that has not been settled yet concerns the risks required by the principal to be undertaken in cases where the agent develops activities in closely related markets. In Daimler Chrysler, the Court suggested that the categorization as an agent in relation to the sale of the principal's goods or services (sale of new cars) does not depend on whether the principal requires the agent to undertake risks in other markets (provision of after-sales servicing and performance of guarantee work on vehicles).[32] This approach is in sharp contrast to the one the Court followed in VAG Leasing where, in deciding whether Article 101 TFEU applied to obligations placed on Volkswagen dealers when they acted as agents entrusted with leasing Volkswagen vehicles, it took into consideration that these dealers were required by Volkswagen to sell and provide after-sales services in their own name and for their own account.[33] Another question that still seeks for a satisfactory answer is whether some risks may be borne by the agent without the relevant obligations jeopardizing the qualification of the relationship as a genuine agency. For instance, in its 1962 Notice on Exclusive Dealing Contracts with Commercial Agents the Commission had accepted that the agents could assume the del credere guarantee[34] whereby the agent acts not only as a salesperson for the principal, but also as a guarantor of credit extended to the buyer. Yet, in VAG Leasing the Court followed a more stringent approach ruling that the agents should not «bear ***any*** of the risks resulting from the contracts negotiated on behalf of the principal» [emphasis added].[35] To make matters more ambiguous, the Commission Guidelines on Vertical Restraints note that Article 101(1) TFEU does not apply if the agent «bears

30 See, for instance, ECJ, Joined Cases 40-48,50, 54-56, 111, 113 & 114/73 Colperarieve Vereniging 'Suiker Unie' UA and others v Commission [1975] ECR-1663, paras. 482 and 541.

31 Commission Guidelines on Vertical Restraints [2010] OJ C 130/01, para. 16.

32 ECJ, Case T-325/01 DaimlerChrysler v. Commission, [2005] ECR II-3319, para. 66.

33 ECJ, Bundeskartellamt v Volkswagen AG and VAG Leasing GmbH, [1995] ECR I-3477, paras. 19-21.

34 Notice on Exclusive Dealing Contracts with Commercial Agents, OJ 1962 139/2921, para. 1.

35 Supra. 33, para. 19. In a more recent case, ECJ Case C-217/05, the Court ruled that «the fact that the intermediary bears only a negligible share of the risks does not render Article 85 [now Article 101] of the Treaty applicable». See para. 61.

only insignificant risks».[36] The Guidelines do not clarify the types of risks and/or the magnitude of financial or commercial responsibility that could be assumed by the agent without the agreement triggering the application of Article 101(1) TFEU.[37]

The second condition is integration of the agent with the principal's business. More particularly, for an agency agreement to render Article 101(1) TFEU inapplicable, the agent should «neither undertake nor engage in activities proper to an independent trader».[38] This criterion (also referred to as criterion of economic dependence) excludes from the favorable regime cases in which the agent acts on behalf of various principals or develops in parallel other commercial activities.[39] However, the extent to which this requirement has been embraced by the Court and the Commission is not clear. More particularly, in the past, Court rulings and Commission decisions have largely been based on whether the agent acted as an «auxiliary organ» of the principal.[40] According to this case law, the agent enjoys limited autonomy with respect to the principal and may not engage in the activities of both agent and independent dealer in respect of the same market.[41] Since the 1990s though, as a result of the shift towards a more economics-based approach in competition law assessments, the case law seems to have mainly focused on how the risks are allocated between agent and principal.[42] However, neither the Court nor the Commission have abandoned the economic dependence/integration criterion altogether[43] and this makes it difficult to say with certainty that an undertaking (even if we assume that it bears no risks), which engages in closely related activities and provides the same services to other principals, would benefit from immunity.

Putting this back into the publishing context, **two** questions seek for answer.

First, could the agreements between Apple and the Publishers escape the Article 101(1) TFEU prohibition? Starting from the condition that the agent should be in-

36 Commission Guidelines on Vertical Restraints [2010] OJ C 130/01, para. 15.

37 Dieny 2008, 7.

38 Notice on Exclusive Dealing Contracts with Commercial Agents, OJ 1962 139/2921, para. 1.

39 See Geradin et al. 2012, 110.

40 See, for instance, supra. 30, paras. 545-546 and European Commission, Pittsburg Corning Europe OJ 1972 L 272/35, para. 38 and Commission, European Sugar Industry OJ 1973 L 140/17.

41 Lianos 2007, 632.

42 For a comprehensive overview of the evolution of the relevant case law see, for instance, Zhang 2013, pp. 565-570 and Lianos 2007, pp. 631-648.

43 See, for instance, Daimler Chrysler, paras. 85-88 and Case C-217/05 Confederacion Espanola de Empresarios de Estaciones de Servicio v. Compania Espanola de Petroleos SA [2006], paras. 42-44. As for the Commission's approach, see one the one hand, the 2010 Commission Guidelines, para. 13 and compare against Commission, Mercedes-Benz OJ 2001 L 257/1, para. 159(d).

tegrated with the principal's business, we are not certain about how the Commission would deal with the fact that Apple sells the books of more than one publisher or that it develops in parallel a considerable amount of other business activities for its own account.[44] As previously noted, it may state in its Guidelines that an entity may qualify as an agent irrespective of whether it acts for one or several principals, but its assessments are not entirely immune from economic dependence considerations. With respect to the second requirement, without access to the agreements, we do not know whether Apple bears no or only insignificant risks. The commitments decision is not helpful in that regard, because it is limited to the description of certain pricing terms of the agreements from which we may not infer whether Apple assumed any responsibilities that would render Article 101(1) TFEU inapplicable.[45] For now, we may only speculate whether Apple would be perceived as a genuine agent for the purposes of EU competition law.

In principle, a narrow interpretation of these criteria would lead to the conclusion that Article 101(1) applies. Besides the fact that this is a case of multiple agency involving a retailer that operates to a large extent independently of one particular publisher, Apple also seems to have incurred some costs to promote the publishers' e-books. For instance, it has created an instrument, the Widget Builder, which allows publishers to increase sales of their books on the iBooks Store by adding interactive widgets to their websites and blogs.[46] If the creation of such an instrument were an obligation under the agency agreement signed with the publishers, it could qualify as a market-specific investment,[47] which, according to the Guidelines, is a type of risk that should not be borne by the agent for the agreement to benefit from the exception.

However, one may wonder whether such a narrow interpretation serves the purposes for which the special competition regime for agencies has been established in the first place. Excluding from said regime multiple agencies[48] or cases where the agent develops a marketing strategy to promote the principal's products[49] would result in preventing almost all agency arrangements from qualifying for immunity. In the case at hand (and online agency structures that have similar characteristics in general), since both owners-

44 This was, for instance, a factor on which the Commission based its decision in Pittsburg Corning Europe [1972] L 272/35, para. 38.

45 Commitments decision, see in particular paras. 31 et seq.

46 http://widgets.itunes.apple.com/builder/ For further investments Apple has made to promote e-authors and publishers see: http://www.apple.com/support/mac-apps/ibooksauthor/

47 According to the Guidelines, para. 14.

48 For this reason, the integration criterion has been severely criticized. See, for instance, Lianos 2007, 634 and Zhang 2013.

49 Bennett 2013, 8-9.

hip of the e-book and price control are in the hands of the publishers, the characterization of the relationship as a genuine agency should not be disregarded.[50]

Second, could granting antitrust immunity to an online agency agreement governing trade in books help advance pluralism in the publishing industry? The answer to this question depends on the particularities of the market in which publishers and e-tailers that have signed the agreement operate. The agency model allows publishers to set the prices at which their books are sold to the end-customer and, in that regard, it greatly resembles «traditional» fixed book pricing arrangements. In principle, fixed book pricing may lead to the production of a wider range and more original books because it allows publishers to subsidize less popular titles by fast-selling books. In other words, fixed prices set by the publisher may offset the risk of publication of more literary books. This is not mere cultural rhetoric, but an argument grounded on economic theory on the efficiencies of retail price maintenance (RPM) and, more particularly, the demand-uncertainty theory, on the basis of which, in cases where there is uncertain consumer demand,[51] manufacturers may take risks more easily if they are allowed to set a minimum price for their products.[52] In other words, with a fixed price mechanism in place, publishers can use the protected high retail margin to sell a more original title to booksellers that the latter would not be willing to buy in a free pricing system. Thus, RPM may prove to be an instrument affording publishers the ability to cross-subsidize titles that carry a certain cultural value but are highly unlikely to cover their costs. The agency model may also contribute to the creation and/or preservation of an extensive network of retailers: In theory, RPM may shield a cartel of low-volume retailers, which use manufacturers to coordinate prices at the retail level, from being pushed out of the market by discount chain stores.[53]

However, these propositions are not always true and related arguments may hold where these positive effects cannot arise in a free pricing system. To put it simply, an agency structure may be preferable to the wholesale model if a variety of books and a wide web of bookstores are not possible to achieve with free prices.[54] Strongly related

50 Ibid., 9.

51 For an interesting analysis of why the success of a book cannot be predicted see Vanderbilt, T. «Why is literary fame so unpredictable?» 21/05/2012 The New Yorker, available at: http://www.newyorker.com/online/blogs/books/2012/05/why-is-literary-fame-so-unpredictable.html.

52 On the demand-uncertainty theory as a justification for RPM see, for instance, Steiner 1985; Butz 1997; Deneckere et al. 1997 and Marvel 1994.

53 Appelman and Canoy 2002, 590-591 referring to Ornstein 1985; For more details on the cartel of retailers hypothesis see, for instance, Areeda and Hovenkamp 2004, 35-68.

54 As the Commission puts it in VBBB/VBVB, para. 52, the publishers' control over prices would lead to these results if the latter «could not reasonably be expected in the in the prevailing industrial and commercial context».

to the discussion over which pricing model is more adequate to protect (both price and non-price) competition in the book market is Amazon's heavy discounts policy and how the latter may have affected content output and the book distribution system. More particularly, as soon as it launched its e-reader Kindle and with a view to boosting sales of the device,[55] Amazon began offering e-books, including newly released English-language bestsellers, to consumers for USD 9,99.[56] This price was not only substantially below the retail price proposed by the publishers, but also below the wholesale price at which Amazon was buying the e-books from them.[57] While empirical research that has been conducted in relation to this issue is scarce, it is worth reflecting on the problems that may arise from this practice.

From the consumers' perspective, this pricing policy may substantially alter book-reading habits. For instance, with Amazon charging such low prices, consumers may refrain from buying books that cost more because this is what they expect any title to cost thereby devaluing the book as a literary creation.

Furthermore, as a result of the fact that e-books cost substantially less than hardcover versions, **publishers face pressure to reduce prices of print books**.[58] This may result in lower prices for the consumers but **a race to the bottom on price may have a negative impact on quality and editorial diversity because in a free pricing system, publishers are not necessarily incentivized to invest in new authors and/or more original titles**. Why is that? Producing a book has large fixed but low distribution costs. In other words, while the costs that a publishing house needs to incur at the creation stage, also referred to as first-copy costs, are high, once the author has written the book, the incremental cost of distribution to an additional consumer is very low.[59] By giving them the opportunity to exploit large economies of scale and of scope, this feature motivates publishers active in a free market to focus on mass-market titles so as to attract as many readers as possible. To put it simply, it is safer for publishers to invest in easily digestible and more of the same («tried recipe») type of content. Thus, free prices may have a negative effect on the production of more original titles.

Finally, **brick-and-mortar shops, which find it difficult to compete with such prices, may be forced to exit the market**.[60] In other words, a heavy discounts policy may

55 Joint Research Center Technical Report on the Book Publishing Industry 2013, 73.

56 In 2011 Amazon's Kindle store offered 950,000 ebook titles, of which 800,000 would cost $9.99 or less. See Wischenbart 2011, 5.

57 Commitments decision, para. 22.

58 Case 1:12-cv-02826-UA United States of America v. Apple Inc; Hachette Book Group; Harper Collins Publishers Inc; Penguin Group (USA) Inc; Simon and Schuster Inc, United States District Court, Southern District of New York), Document 1, (Complaint), filed 11/04/2012, p. 9.

59 Goodman 2004, 1432-1434.

60 OECD Report on E-books: Developments and Policy Considerations 2012, p. 28.

shut down «a show-room for books, thus further narrowing the venues where consumers can see and learn about new reading materials».[61] In its turn, this may adversely affect book reading, particularly in older age groups that seem to prefer the traditional channel to the Internet.

Yet, in order to draw conclusions as to whether the above assumptions may be materialized with a free pricing system, further empirical research is required. Studying this issue more profoundly has become imperative in that online agency structures are starting to play a major role in the current media landscape. For instance, in the book industry, following Apple, major online retailers Amazon, Barnes & Noble, Kobo and Sony have concluded agency agreements with publishers for the sale of e-books. Newspaper publishers and film studios have also embraced this model.[62] In the app market, Google has adopted an agency model identical to the one used by Apple.[63] It is therefore clear that resale price maintenance has become a rather popular strategy in media markets affecting both the price of the content per se (e.g. in the case of newspapers) and the price of the instruments that are needed to access such content (e.g. in the case of apps required to read the online version of a newspaper).

3.2. How could «false» agency agreements be granted an exemption under Article 101(3) TFEU?

In cases where a contractual relationship does not qualify as a genuine agency, it may still benefit from an exemption under Article 101(3) TFEU. The question then arises how Article 101(3) TFEU can be applied to «false» agency agreements with a view to promoting a pluralistic book market.

With respect to the first requirement set by Article 101(3) TFEU that the agreement must contribute to improving the production or distribution of goods, it has already been mentioned that fixed prices may lead to the production of more original titles because they enable publishers to offset to some extent the costs of books that are not very attractive commercially against the profits made on those printed in large number. As regards improvements in distribution, an agency model may contribute to the creation of an extensive network of e-tailers which, under a free-pricing system, may be discouraged from entering a market dominated by large retailers with significant bargaining power and resources at their disposal. In its turn, a wide web of e-tailers

61 See http://publishingtrendsetter.com/industryinsight/simple-explanation-agency-model/.

62 See, for instance, Kahn, J. «Cue on agency model: 'I don't think you understand. We can't treat newspapers or magazines any differently than we treat Farm Ville», 23/04/2012, available at: http://9to5mac.com/2012/04/23/cue-on-agency-model-i-dont-think-you-understand-we-cant-treat-newspapers-or-magazines-any-differently-than-we-treat-farmville/.

63 See https://support.google.com/googleplay/android-developer/answer/112622?hl=en.

collaborating with different publishers may «allow a number of titles which may never have been made into e-books to be sold in the digital marketplace».[64]

A «false» agency arrangement may also fulfil the fourth condition set by Article 101(3) TFEU that the agreement must not afford the parties the possibility of eliminating competition in respect of a substantial part of the products in question: Since competition on the upstream level is driven by the originality of the content produced by the author and price competition is relevant for a limited number of books that have close substitutes (e.g. dictionaries, travel guides cookbooks, etc.), then agreements that preclude price competition at the retail level do not result in an elimination of competition in a substantial part of the products under consideration thereby being eligible for an exemption under Article 101(3) TFEU.

As for the condition that the agreement must allow consumers a fair share of the resulting benefit, it should be pointed out that the agency model does not necessarily lead to higher prices for the end-consumer. For instance, Foros et al. developed a model which shows that, in the prevailing e-book market context where the degree of competition is higher at the upstream level than at the downstream level, prices are lower with than without an industry-wide adoption of the agency mechanism.[65]

Finally, with respect to the indispensable nature of the agency mechanism to secure the production of a wide variety of books or an extensive network of retailers carrying a broad range of titles, the assessment should not be limited to the e-book universe, but consider the book economy in general. Otherwise, the analysis runs the risk of drawing erroneous conclusions. That being said, it may be essential for publishers to adopt the agency model for the sale of e-books, because control over prices may be the only way to increase sales through the traditional distribution system (and, arguably, their total revenues thereby allowing the production of more original books). This is particularly when online sales have an adverse effect on demand in the traditional channel. In such market context, entering into an agency relationship may also be key to the survival of the e-tailer. Abhishek et al. have illustrated why this may be the case. In the event that e-sales have a negative impact on sales through the traditional channel, the publisher has the incentive to limit e-sales.[66] If a wholesale arrangement is made, the publisher will set a high wholesale price for the e-tailer which will ultimately result in higher retail prices. In other words, where online sales have an adverse effect on demand in the traditional

64 Campbell, M., «DOJ e-books trial: Apple's Cue explains 'agency' contracts and pricing, denies culpability», 17/06/2013, in Apple Insider, referring to comment made by Apple's senior vice president of Internet Services and Software Eddy Cue available at: http://appleinsider.com/articles/13/06/17/doj-e-cooks-trial-apples-cue-explains-agency-contracts-and-pricing-denies-culpability.

65 Foros 2012, 10-14.

66 Abhishek et al. 2013, 15-16.

channel, agency agreements may be indispensable to securing the efficiency of the e-channel.[67] It should be pointed out that the issue of how e-book sales affect sales at the brick-and-mortar stores is far from settled and further empirical research is needed to reach more definitive conclusions.

To sum up, an elaborate approach to agency arrangements under Article 101(3) TFEU as the one suggested above may reveal that a «false» agency may not only lead to lower prices for e-books and e-readers, but also contribute to the preservation of the traditional distribution network, which older generations prefer, and stimulate competition in titles on both the upstream and (online) downstream levels of the supply chain.

4. AGENCY IN THE POST-COMMITMENTS PERIOD

Having discussed the questions that the Commission abstained from answering in the E-books decision, we will now turn to the issue that was addressed therein that is, the way the involved firms committed to behave in order to address the Commission's concerns. As previously mentioned, the Commission did not oppose the agency model as a business strategy to sell e-books. On this basis, while the decision imposes upon the Publishers the obligation to «terminate their respective agency agreements for the sale of books in the EEA concluded with Apple»,[68] it also clarifies that each of the Publishers and Apple «remain free to enter into agency agreements in line with the final commitments in so far as those agreements and their provisions do not infringe Union competition legislation».[69] A few months later, Harper Collins and Hachette became the first publishers involved in the case to conclude agency agreements with Amazon[70] with Simon & Schuster following shortly thereafter.[71]

These new agreements have been referred to as «refined» to highlight the fact that they have been drafted in conformity with the commitments decision. The main undertaking consists in that, for a two-year («cooling-off») period, each of the publishers may not prevent an e-book retailer from setting or altering prices of e-books. More particularly, the publishers may still sign agency agreements provided that they do not interfere with the e-tailers' freedom to «***reduce the retail prices of e-books by an aggregate***

67 Ibid. See also Condorelli et al. 2013 who reach a similar conclusion.

68 Commitments decision, paras. 97 and 130.

69 Ibid., para. 153.

70 Campbell, L. «Harper Collins and Hachette UK Refine Agency Model», 03/04/2013, The Bookseller, available at: https://thebookseller.com/news/hc-and-hachette-uk-drop-agency-model.html.

71 Pilkington, M., «Simon & Schuster Adopts Refined Agency Pricing with Amazon UK», 29/04/2013, The Good E-reader, available at: http://goodereader.com/blog/electronic-readers/simonschuster-adopts-refined-agency-pricing-with-amazon-uk.

amount equal to the total commission the publisher pays to the e-book retailer, over a period of at least one year […] and/or to use that amount to offer any other forms of promotions».[72] Thus, in the post-commitments period, retailers may compete on price without the publishers being able to object to their discounts policies (no matter how aggressive they are). However, one may wonder whether this solution may effectively address the problems that were discussed above. It seems that, by undertaking to allow retailers to offer books at lower prices, publishers are not significantly affected in that they possess significant bargaining power against small retailers and can therefore reach an agreement that enables them to exercise a high degree of control over retail prices. Yet, this does not automatically mean that publishers will direct the profits they make from titles that sell well to the production of more literary books. Price control might as well lead to publication of mass-market titles and, for this reason, it should not be assumed that accepting this commitment helps advance pluralism on the upstream level.

Furthermore, since the burden is placed on the retailers to reduce prices (by an amount equal to their total commission), pluralism at the retail level is also at stake. This is a concern that was raised in the context of the consultation the Commission conducted to market test the undertakings suggested by the parties. More particularly, interested stakeholders drew the Commission's attention to the market power Amazon would acquire if this commitment were accepted. Yet, while the Commission acknowledged that «larger retailers may have certain advantages over smaller retailers, including economies of scale»,[73] it abstained from considering both the effects of the proposed solution on supply diversity at the retail level and the wider ramifications of an Amazon monopoly for the industry. It is submitted here that not only should the Commission take into account Amazon's position in the market for e-books but also its position in the market for e-readers, including related advertising/promotional mechanisms, and the rather profitable activities it has started to develop as a provider of independent publishing services.[74] With that said, having in mind the negative impact of vertical integration on competition for titles and access to bookshelves, the Commission's narrow approach in this case, aiming at restoring (probably only temporarily) price competition, is short-sighted to say the least.

Finally, and related to the above, while interested stakeholders have also raised an argument about the effects of the proposed solution on cultural diversity, the Commission was limited to replying that «***the purpose*** of the Final Commitments by each of the Four Publishers and Apple ***is to restore as much as possible the conditions of competition***

72 Commitments decision, paras. 99-100.

73 Ibid., para. 151.

74 On how to publish with Amazon see: http://www.amazon.com/gp/seller-account/mm-summary-page.html?topic=200260520.

that existed prior to the possible concerted practice. The Commission considers that ***in making those commitments binding, it is not adversely affecting cultural diversity*** in the EEA».[75] This hands-off approach in relation to non-economic concerns is problematic since, absent any analysis of whether and if so, how and to what extent the undertaking in question could affect cultural diversity, ignores the public utility components of the book and renders Article 167(4) TFEU (establishing the Commission's obligation take media pluralism into account in the implementation of the EU competition policy) a dead letter.

5. CONCLUSIONS

In the E-Books case, the Commission does not condemn the agency model, but does not embrace it either. It is submitted in this paper that, irrespective of whether an agency arrangement qualifies as «genuine» or «false», the Commission's analysis in subsequent cases needs to take account of the effects of aggressive price competition not only on the quality of the books produced, but also on the traditional distribution channel, whose survival is of utmost importance to older generations. The commitment that was accepted by the Commission in the E-Books case, on the basis of which the publishers may still sign agency agreements provided that they do not prevent retailers from offering discounts by an amount equal to their commission, is far from appropriate to address either competition or pluralism concerns that have arisen in the book market. It is clear that the Commission's only objective was to reintroduce price competition at the expense of a wide web of retailers that could allow a wider variety of titles to be sold in (both the off- and online) book markets. This approach converges with the one adopted by the Commission in the early days of its antitrust practice in the field and leads to the conclusion that it has treated books like any other marketable commodity thereby undermining their role in advancing broader societal goals.

6. BIBLIOGRAPHY

Abhishek, V., Kinshuk Jerath and Z. John Zhang. 2013. Agency Selling or Reselling? Channel Structures in Electronic Retailing.

Allan, W. and Curwen, P. 1991. Competition and Choice in the Publishing Industry. London: Institute of Economic Affairs.

Appelman, M.D. and Canoy, M.F.M. (2002), 'Horses for Courses – Why Europe Should Not Harmonise Its Book Policies', 150 De Economist 5, 583-600.

75 Commitments decision, para. 152. See also para. 127.

Areeda, Phillip E. and Herbert Hovenkamp. 2004. Fundamentals of Antitrust Law, 2nd ed., New York: Aspen Publishers Inc.

Bennett, M. 2013. Online Platforms: Retailers, Genuine Agents or None of the Above? Available at: https://www.competitionpolicyinternational.com/online-platforms-retailers-genuine-agents-or-none-of-the-above

Brynjolfsson, E., Yu (Je_rey) Hu, and Mohammad S. Rahman. 2009. Battle of the Retail Channels: How Product Selection and Geography Drive Cross-Channel Competition. Management Science, 55(11): 1755-1765.

Butz, D. «Vertical Price Controls with Demand Uncertainty,» Journal of Law and Economics, 40:2, October 1997, 433-459

Case 1:12-cv-02826-UA United States of America v. Apple Inc; Hachette Book Group; Harper Collins Publishers Inc; Penguin Group (USA) Inc; Simon and Schuster Inc, United States District Court, Southern District of New York), Document 1, (Complaint), filed 11/04/2012.

Campbell, M., «DOJ e-books trial: Apple's Cue explains 'agency' contracts and pricing, denies culpability», 17/06/2013, in Apple Insider, referring to comment made by Apple's senior vice president of Internet Services and Software Eddy Cue available at: http://appleinsider.com/articles/13/06/17/doj-e-cooks-trial-apples-cue-explains-agency-contracts-and-pricing-denies-culpability

Condorelli, D., Andrea Galeottizand and Vasiliki Skreta. 2013. Selling Through Referrals. Working Paper. Available at: https://economics.wustl.edu/files/economics/imce/draft_25_ilari2.pdf

Deneckere, R., H. P. Marvel, and J. Peck, «Demand Uncertainty and Price Maintenance: Markdowns as Destructive Competition,» American Economic Review, 87:4, September 1997, 619-641.

Fishwick, F. (2008), 'Book Prices in the UK since the End of Resale Price Maintenance', 15 International Journal of the Economics of Business 3, 359-77.

Foros, O., Hans Jarle Kind and Greg Shaffer. 2012. Turning the page on business formats for digital platforms : does Apple's agency model soften competition? Available at: http://www.econbiz.de/Record/turning-the-page-on-business-formats-for-digital-platforms-does-apple-s-agency-model-soften-competition-foros-oystein/10009786199.

Geradin, D., Dr Anne Layne-Farrar, and Nicolas Petit. 2012. EU Competition Law and Economics. Oxford: Oxford University Press.

Gippini-Fournier, E. 2009. Resale Price Maintenance in the EU: In Statu Quo Ante Bellum? Fordham Corp. L. Inst - 36th Annual Conference on International Antitrust Law and Policy, 2009 (B. Hawk ed., 2010). Also available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1476443.

Goodman, Ellen. 2004. Media Policy Out of the Box: Content Abundance, Attention Scarcity, and the Failures of Digital Markets, 19 BERKELEY TECH. L. J. 1389.

Goolsbee, A. 2001. Competition in the Computer Industry: Online versus Retail. The Journal of Industrial Economics, 49(4):pp. 487-499.

Grienfield, J. Kindle Most Popular Device For Ebooks, Beating Out iPad; Tablets On The Rise, Forbes 30/10/2013, available at: http://www.forbes.com/sites/jeremygreenfield/2013/10/30/kindle-most-popular-device-for-ebooks-beating-out-ipad-tablets-on-the-rise/

Hilton, J. and David Wiley. 2010. The Short-Term Inuence of Free Digital Versions of Books on Print Sales. The Journal of Electronic Publishing, 13 (1).

Lianos, I. 2007. Commercial agency agreements, vertical restraints, and the limits of article 81(1) ec: between hierarchies and networks. Journal of Competition Law & Economics, 3 (4) 625-672.

Linklater, E. 2013. *Working Paper*. Florence: European University Institute.

Marvel, Howard (1994), «The Resale Price Maintenance Controversy: Beyond The Conventional Wisdom», 63 Antitrust L. J. 59. Notice on Exclusive Dealing Contracts with Commercial Agents [1962] OJ 139/2921.

OECD. 2012. Report on E-books: Developments and Policy Considerations.

Orbach, B. Y. 2008. 'Antitrust Vertical Myopia: The Allure of High Prices' (2008) 50 *Arizona Law Review* 261-287 (Arizona Legal Studies Discussion Paper No 07-25, SSRN).

Ringstad, V. (2004), 'On the Cultural Blessings of Fixed Book Prices', 10 International Journal of Cultural Policy 3, 351-65.

Smith, M. D. and Rahul Telang (2010) Piracy or Promotion? The Impact of Broadband Internet Penetration on DVD Sales. Information Economics and Policy, 22(4):289-298. Special Issue: Digital Piracy.

Steiner, R. L (1985) The Nature of Vertical Restraints. The Antitrust Bulletin (30): 143-197.

Stockmann, D. (2004), 'Free or Fixed Prices on Books - Patterns of Book Pricing in Europe', 11 Javnost - The Public 4, 49-64.

UK Restrictive Practices Court, Judgment «In the matter of the Restrictive Trade Practices Act 1976 and in the matter of the Net Book Agreement 1957 and in the Matter of the Resale Prices Act 1976 and in the matter of books and related classes of goods» Judgement of Ferris, J. 1997.

Utton, M.A. (2000), 'Books Are Not Different after All: Observations on the Formal Ending of the Net Book Agreement in the UK', 7 International Journal of the Economics of Business 1, 115-26.

Vedder, H.H.B. 2003. Competition Law and Environmental Protection in Europe; Towards Sustainability? Europa Law Publishing: Groningen.

Van der Ploeg, F. (2004), 'Beyond the Dogma of the Fixed Book Price Agreement', 28 Journal of Cultural Economics, 1-20.

Wischenbart, R. and Carlo Carrenho, Veronika Licher, Miha Kovac and Vinutha Mallya. 2011. Global eBook Report: Current Conditions & Future Projections. For an updated version see: http://www.wischenbart.com/upload/The%20Global%20eBook%20Report%202013_Findings_01.pdf

Zhang, H. 2013. Toward an Economic Approach to Agency Agreements. Journal of Competition Law and Economics, 9(3), 553-591.

ANÁLISIS JURÍDICO DE LOS PROBLEMAS DERIVADOS DEL *SCREEN SCRAPING* REALIZADO CON FINES COMERCIALES. EXAMEN DESDE LA PERSPECTIVA DEL DERECHO CONTRACTUAL, LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Y LA NORMATIVA REPRESORA DE LA COMPETENCIA DESLEAL

Gemma Minero Alejandre
Profesora Ayudante de Derecho Civil,
Universidad Autónoma de Madrid

RESUMEN: En la presente comunicación se analizan los distintos problemas jurídicos derivados del uso de la denominada técnica del screen scraping, y se hace desde una triple perspectiva: el estudio de las condiciones generales de la contratación previstas en las páginas web del empresario, las peculiaridades de la protección de las páginas web por la propiedad intelectual y la aplicación de la normativa sobre competencia desleal. Para ello se realiza un detallado examen de la más reciente jurisprudencia que ha prestado atención a estas cuestiones. Jurisprudencia que tiene su origen en un supuesto de hecho común: la infracción de las condiciones de navegación impuestas por el titular de la página web, en las que impide a terceros el uso de la técnica del screen scraping para la extracción de los contenidos de su página web. Las partes de los litigios hasta ahora resueltos son también coincidentes: el titular de la página web demandante se trata de una compañía aérea low cost y el tercero infractor de las condiciones de navegación es una agencia de viajes on-line o un buscador de vuelos en línea. El petitum del primero, la condena al pago de la correspondiente indemnización de los daños y perjuicios producidos, junto con la prohibición de continuación del uso de los datos de su negocio, se argumenta desde la triple perspectiva mencionada. La pregunta a contestar es la siguiente: ¿es lícita la oferta o información de los vuelos de una compañía aérea por parte de agencias de viajes on-line o buscadores en línea, junto con el cobro de una comisión, cuando la primera compañía no sólo no ha dado su consentimiento sino que se ha opuesto expresamente a ello en las condiciones de uso de su página web? La respuesta a esta cuestión pasa, en primer lugar, por la aplicación a productos de Internet de los principios básicos del derecho contractual, como es la necesidad de oferta y aceptación para que pueda nacer el contrato.

PALABRAS CLAVE: Condiciones de uso de una página web, condiciones generales de la contratación, (in)existencia de contrato tácito, bases de datos, competencia desleal.

1. ALGUNAS CONSIDERACIONES ACERCA DEL *SCREEN SCRAPING*. INTRODUCCIÓN AL PROBLEMA Y PERSPECTIVAS DEL ANÁLISIS JURÍDICO

La técnica del *screen scraping*, también llamada *web scraping,* que podemos traducir al español como «raspado de pantalla», consiste en el uso de un programa informático que permite introducirse en tiempo real en la página web de un tercero, extraer los datos solicitados por el cliente del segundo sitio web y mostrárselos a este último como datos o contenidos propios, dentro del segundo sitio web. Cuando hablamos de servicios en línea, ello permite la creación de buscadores de servicios y productos, que permiten la contratación de éstos mediante la segunda página web, que cobrará una comisión sobre el precio marcado en la primera página web o cargo de emisión. El precio del producto o servicio exigido por el titular de la primera página web irá directamente a ese titular, de manera que la compraventa del bien o la contratación de producto será directa, pues se llevará a cabo entre los clientes del buscador y el titular de la primera página web, cumpliendo el sitio web del buscador o comparador de precios únicamente una función de intermediación.

Si bien este tipo de sitios web pueden hacer aumentar el número de productos vendidos o servicios contratados, no a todo titular de una página web le tiene por qué interesar que un tercero oferte sus productos o servicios con un sobreprecio. Además, por razones de negocio, las agencias de viajes o buscadores *on-line* suelen ocultar la verdadera identidad de la compañía con la que sus clientes están contratando esos servicios o productos durante el proceso de contratación, luego no es hasta después de la perfección del contrato cuando dicha identidad se desvela.

Las implicaciones jurídicas de esta técnica se discuten a raíz de una batería de demandas planteadas en 2008 y 2009 por *Ryanair* contra las principales agencias de viajes *on-line –Rumbo, Edreams y Atrápalo–*.[1] *Ryanair* entiende que este tipo de prácticas de agencias *on-line* suponen un obstáculo para su modelo de negocio *low cost*, consistente en la venta directa de billetes de avión a bajo coste a través de su propio sitio web para reducir costes de intermediación.

Las citadas acciones han dado lugar a dos sentencias del Tribunal Supremo, ambas de 2012, con las que se pone fin a los litigios que enfrentaban a *Ryanair* con *Edreams*, por un lado, y a *Ryanair* con *Atrápalo*, por otro, y en las que el Alto Tribunal analiza por primera los problemas jurídicos dimanantes del uso de esta técnica. Hablamos de las

1 Demandas que se interponen tanto en España como en otros países europeos, y que han dado lugar a las sentencias del Oberlandesgericht de Frankfurt am Main de 5 de marzo de 2009, del Tribunal de Grande Instance de París, 3 ème chambre, 2ème section, de 9 de abril de 2010, y de la Irish High Court de 26 de febrero de 2010, entre otras.

sentencias del Tribunal Supremo, Sala de lo Civil, Sección 1ª, núm. 572/2012, de 9 de octubre, y 630/2012, de 30 de octubre.[2] Mediante la técnica del *screen scraping, Edreams* y *Atrápalo*, cada vez que un cliente le pide información sobre vuelos desde su página web, le muestran los resultados que *Ryanair* y otras compañías aéreas ofrecen en sus respectivas páginas web, permitiendo su ordenación por precios. Para ello, los buscadores de *Edreams* y *Atrápalo* acceden a la página web de *Ryanair* como si de cualquier usuario común se tratara y extraen la información que les había solicitado el cliente –vuelos programados para una fecha concreta o para un rango de días–. Los buscadores de *Edreams* y *Atrápalo* capturan los detalles de los vuelos publicados en la página web de *Ryanair* y proyectan el resultado en su sitio web –de *Edreams* y de *Atrápalo*–, en la pantalla correspondiente a la búsqueda solicitada, sin hacer mención del origen de esos datos. En sus acciones contra las agencias de viajes *on-line*, la compañía aérea alega como argumento principal una infracción contractual derivada del incumplimiento de los términos o condiciones de uso de su página web, en las que se prohíbe el uso comercial de la información sobre sus vuelos. Asimismo denuncia una infracción de derechos de propiedad intelectual, concretamente del derecho *sui generis* sobre la base de datos que contiene la información sobre sus vuelos y del derecho de autor sobre el programa de ordenador empleado en la búsqueda de vuelos y precios. Finalmente, *Ryanair* invoca también la normativa sobre competencia desleal, al entender que se producen imitaciones desleales, aprovechamiento de su reputación y de su esfuerzo y obstaculización de la posición competitiva que esta empresa ocupa en el mercado.

A todo ello se deben sumar otros dos litigios que acogen la postura de los buscadores y agencias de viajes *on-line*, que aún no han sido analizados por el Tribunal Supremo. Hablamos en este caso de la SAP de Madrid (sección 28ª) de 13 de enero de 2012 y la SAP de Barcelona (sección 15ª) de 21 de mayo de 2012.[3] En ambas resoluciones se analizaba si las conductas que *Rumbo,* en el primer caso, y *Edreams,* en el segundo,

2 SSTS núm. 572/2012 y 630/2012, respectivamente. La primera STS, de 9 de octubre, resuelve el recurso de casación interpuesto por Ryanair contra la SAP de Barcelona, sección 15ª, de 15 de diciembre de 2009, que, a su vez, resolvía el recurso de apelación interpuesto por esta compañía contra la sentencia del Juzgado de lo Mercantil núm. 2 de Barcelona de 21 de enero de 2009. La segunda STS citada, de 30 de octubre de 2012, resuelve el recurso de casación que Ryanair interpuso contra SAP de Barcelona, sección 15ª, de 17 de diciembre de 2009, sentencia núm. 429/2009, que resolvía el recurso de apelación de esta compañía aérea contra la sentencia del Juzgado de lo Mercantil núm. 2 de Barcelona de 11 de febrero de 2009. El litigio entre Rumbo y Ryanair no ha sido resuelto aún por el Tribunal Supremo. La última sentencia dictada en este pleito es la de la Audiencia Provincial de Madrid (sección 28ª) de 30 de marzo de 2012, sentencia núm. 111/2012, en la que se resolvía el recurso de apelación planteado por Ryanair contra la sentencia del Juzgado de lo Mercantil núm. 5 de Madrid de 30 de noviembre de 2010, que desestimaba la demanda contra Rumbo.

3 Sentencias núm. 8/2012 y 208/2012, respectivamente.

imputaban a *Ryanair* merecían o no el reproche de deslealtad. Estas acciones judiciales se basan en el anuncio por parte de *Ryanair* en varios medios de comunicación de su intención de cancelar las reservas realizadas por pasajeros a través de agencias *on-line*, y en la introducción en las condiciones generales de contratación, publicadas en la página web de *Ryanair,* de una cláusula en la que se informaba de un supuesto derecho de cancelación por parte de Ryanair de toda reserva de vuelos realizada desde otra página web, sin previo aviso y sin reembolso. Los órganos de primera instancia entendieron que constituyen actos de obstaculización contrarios a la Ley de Competencia Desleal las manifestaciones realizadas por *Ryanair* difundidas por los medios de comunicación.[4] Los recursos de apelación presentados por *Ryanair* bien merecen la calificación, en sentido material, de auténticas demandas, a la luz de la lista de conductas que *Ryanair* imputa a *Edreams* y *Rumbo*, acompañados también de un reproche de deslealtad, fueron desestimadas en segunda instancia. En sus sentencias, las Audiencias Provinciales aclaran la imposibilidad de juzgar por parte de las Audiencias Provinciales, al hilo de la resolución de la apelación, las conductas de deslealtad que *Ryanair* imputa a *Edreams*, salvo en la medida necesaria para juzgar sus propias conductas, siento en el proceso de apelación objeto de enjuiciamiento únicamente las conductas que *Edreams* y *Rumbo* imputan a *Ryanair*. En el tratamiento de las tres perspectivas sobre las que versa nuestro trabajo –Derecho contractual, protección de la propiedad intelectual y normativa represora de la competencia desleal– utilizaremos como hilo conductor las SSTS de 9 y 30 de octubre de 2003, y, con ello, la contestación dada por el Alto Tribunal a la triple argumentación defendida por *Ryanair* en las distintas estancias.

4 En el Auto del Juzgado de lo Mercantil núm. 1 de Madrid, de 3 de septiembre de 2008, a instancia de Rumbo, se adoptaron medidas cautelares amparadas en el art. 727.7º LEC contra Ryanair, por entender que concurría un comportamiento discriminatorio contra los usuarios que hubieran reservado sus vuelos en agencias en línea respecto a los que lo hubieran hecho directamente en la página web de Ryanair (art. 16.1 de la Ley de Competencia Desleal), y denigración contra Rumbo por las calificaciones utilizadas por Ryanair en sus declaraciones en los medios de comunicación («parásito del sector» y «robo al consumidor», entre otras) (art. 9 de la Ley de Competencia Desleal). En la misma línea, en sentencia del Juzgado de lo Mercantil núm. 1 de Madrid de 13 de septiembre de 2010 se declara que Ryanair ha cometido conductas de obstaculización y acciones denigratorias, contrarias a la Ley de Competencia Desleal (arts. 5 y 9). En la citada SAP de Madrid de 13 de enero de 2012, la estimación del recurso de apelación interpuesto por Rumbo conllevó, además, la calificación de las actuaciones llevadas a cabo por Ryanair como actos de discriminación en materia de condiciones de venta, prohibidos por el art. 16.1 de la Ley de Competencia Desleal.

2. EL *SCREEN SCRAPING* DESDE LA ÓPTICA DEL DERECHO CONTRACTUAL. REFLEXIONES ACERCA DE LA CALIFICACIÓN JURÍDICA DE LAS CONDICIONES DE ACCESO A UN SITIO WEB IMPUESTAS POR SU TITULAR Y LA INFRACCIÓN DE ÉSTAS

A la vista de su modelo de negocio, basado en la comercialización directa de sus billetes a través de su página web o su centro de llamadas, *Ryanair* hace públicas en su sitio web una serie de condiciones de uso y advierte que únicamente autoriza el uso de esa página web al usuario que respete efectivamente esas condiciones. Entre ellas, la tercera condición, bajo el rótulo *«Uso permitido»*, establece: *«No se permite utilizar esta página web para cualquier propósito que no sea el uso privado y no comercial. Queda prohibido el uso de cualquier sistema o software automatizado para extraer datos de esta página web para fines comerciales (adquisición de datos o «screen scraping»). Ante el uso indebido y no autorizado de la presente página web, Ryanair se reserva el derecho a ejercitar las acciones que considere oportunas, incluso a instar procedimientos judiciales sin previa notificación». Por su parte, la quinta cláusula, «Enlaces al sitio web», declara: «No se permite establecer ni gestionar enlaces a este sitio web sin el previo consentimiento por escrito de Ryanair»*.

Teniendo en cuenta estas condiciones de uso, *Ryanair* alega la existencia de un contrato entre esta compañía y los usuarios de Internet que visitan su sitio web. Contrato que considera incumplido por las demandadas, sustentando su pretensión en los arts. 5.3 y 5.4 en la Ley sobre Condiciones Generales de la Contratación. *Ryanair* se aferra al argumento basado en el concepto de *browse wrapping*, esto es, en el perfeccionamiento o la existencia de un contrato por el solo hecho de la navegación por la página web, utilizando sus contenidos y aplicaciones, y, por ello, aceptando las condiciones impuestas por el titular de la página web. En segundo lugar, *Ryanair* afirma que *Edreams* y *Atrápalo* hacen uso efectivo de la web, pues son las agencias de viajes las que se ocupan de dar por aceptadas las condiciones de uso en el proceso de perfección de los contratos, marcando las correspondientes casillas de aceptación para completar la reserva por cuenta de sus clientes, que no acceden directamente a la página web de *Ryanair*.

Esta primera pretensión no ha sido acogida por ninguna de las sentencias dictadas hasta la fecha de cierre de este trabajo, a las que nos hemos referido en el anterior epígrafe. En las tres instancias se afirma que, aunque resulte evidente que *Edreams* y *Atrápalo* no respetan las condiciones de uso de la página web de *Ryanair*, dicho comportamiento no puede calificarse como incumplimiento contractual por la sencilla razón de que entre ambos (*Ryanair*, como titular de la página web, y *Edreams*, como usuario de ésta, en primer lugar, y *Ryanair* y *Atrápalo*, en los mismos términos, en segundo lugar) no media relación contractual alguna, pues no se puede afirmar que se concluya un contrato tácito ni una licencia implícita por el mero uso de un sitio web.

En este sentido, el Tribunal Supremo, tras calificar como cuestión de hecho la apreciación de la existencia o inexistencia de consentimiento expreso y, en definitiva, de

contrato –y, con ello, la exclusión de su examen de los fines de la casación– aclara que las sentencias recurridas no rechazan la posibilidad abstracta de que la información sobre las ofertas pueda ser objeto de un contrato ni de que el propio acceso a las ofertas pueda condicionarse por la vía de un contrato regulador de tratos previos. Por tanto, se admite la posibilidad de que el titular de un sitio web introduzca una serie de condiciones que operen como oferta contractual que pueda ser aceptada al navegar por esa página. Lo que las sentencias afirman es que no existe contrato entre *Ryanair* y *Edreams* y entre *Ryanair* y *Atrápalo* y, por ello, no hay infracción contractual derivada del incumplimiento de las condiciones generales de uso de la página web de la demandante. En otras apalabras, una cosa es introducir en una página web una oferta contractual y otra muy distinta es pretender defender que cualquiera que navegue por esa página se convierte en parte contractual, cuando el titular de esa página web no tiene medios técnicos para impedírselo. *«[N]o puede confundirse la infracción de un contrato –que exige la previa prestación de consentimiento– con la actuación de quien, con rechazo más o menos expreso de las condiciones impuestas por el titular de una web y, por vía de hecho, a modo de atajo o pasarela facilita a los consumidores finales el acceso directo a determinados contenidos de la web, sin necesidad de seguir el itinerario de navegación diseñado por su titular, durante el cual se ofertan al usuario pluralidad de productos o servicios más o menos relacionados con el vuelo que el consumidor final pretende contratar y que no podrán ser aceptadas al ser desconocidas»*.[5]

Este pronunciamiento no es uniforme a nivel europeo. Algunos tribunales nacionales han fallado en un sentido similar al seguido por nuestro Tribunal Supremo.[6] Otros, sin embargo, han reconocido que las condiciones de uso de la página web de *Ryanair*, publicadas en su sitio web, y la navegación por éste por parte de las agencias de viajes dan lugar al nacimiento de una relación contractual entre ambas partes.[7]

Vale la pena detenernos en el examen del cumplimiento de lo dispuesto en los apartados tercero y cuarto del art. 5 de la Ley de Condiciones Generales de la Contratación. Tal y como CARBAJO CASCÓN ha señalado,[8] un supuesto como éste cumpliría lo dispuesto en el art. 5.3 de ese cuerpo legal, que exige que el predisponente anuncie las condiciones generales en un lugar visible dentro del lugar en que se celebra el negocio o

5 STS de 30 de octubre de 2012, FJ 2º, párrafo 32.

6 El Tribunal de Grande Instance de París en sentencia de 9 de abril de 2010, asunto Ryanair v. Vivacances y la Corte de Hamburgo, en sentencia de 28 de agosto de 2009, asunto Ryanair v. Vtours.

7 Así, la sentencia de la High Court of Ireland de 26 de febrero de 2010, asunto Ryanair Ltd contra Billigluege.de GmbH [(2010) IEHC 47]. Véase GARCÍA VIDAL, A. (2013). Problemas jurídicos derivados del uso del screen scraping, Sentencia (Sala de lo Civil, Sección 1ª) núm. 572/2012, de 9 de octubre, Cuadernos Civitas de Jurisprudencia Civil, 92, 343.

8 CARBAJO CASCÓN, F. (2010). cit., 605.

que, de cualquier otra forma, garantice al adherente una publicidad efectiva de conocer su existencia y contenido en el momento de la celebración, pero no cabe afirmar lo mismo en relación con las condiciones previstas en el art. 5.4 de la Ley de Condiciones Generales de la Contratación. En efecto, esta norma, que regula el uso de condiciones generales en contratos electrónicos, exige que conste la aceptación de todas y cada una de las clausulas del contrato, sin necesidad de firma convencional, enviándose inmediatamente al consumidor justificación escrita de la contratación efectuada incluyendo todos los términos de la misma –son los denominados contratos *click-wrap* o *web-click*–. Las condiciones de clara significación declarativa y envío de confirmación de la contratación efectuada no se cumplen en nuestro caso.

En el otro extremo debemos indicar que un sector doctrinal español sí defiende la teoría de la *facta concludentia*, es decir, de la posibilidad de aceptación del contrato por actos concluyentes, siempre que se pueda inducir la existencia de un consentimiento o pueda ser relativamente frecuente o habitual en esa forma de contratación.[9] Manifestación de actos concluyentes que se desprenden de actos como el pago a través de la página web. Sin embargo, debemos llamar la atención sobre el objeto de la pretensión de *Ryanair,* que no se refiere al acto de pago, sino a la existencia de relación contractual por el mero hecho de la navegación en su página web. En este sentido, sí nos parece adecuada la aplicación de la postura jurisprudencial antes expuesta, que pasa por la exclusión de la viabilidad del contrato de licencia implícita en nuestro ordenamiento en supuestos de clara falta de inexistencia de significación declarativa del usuario de Internet a favor de la contratación.

Más allá de ello, o tras la asunción de la inexistencia de contrato entre el titular de la página web y cualquiera de los usuarios de Internet, conviene preguntarse cuál es la eficacia –si es que hay alguna– de las condiciones de uso predispuestas unilateralmente por el titular de una página web. La respuesta creemos que ha de ser negativa, con la consiguiente imposibilidad del titular de la página web de hacerlas valer frente a los usuarios que las incumplan. Ante la equiparación que *Ryanair* hace entre el derecho de admisión del propietario de un establecimiento público y la posibilidad del titular de una página web de establecer las condiciones de acceso y uso de ésta, la Audiencia Provincial de Barcelona se hace eco de la contradicción existente entre ofrecer el acceso abierto y libre, sin ningún tipo de restricción, a su sitio web y posteriormente pretender discriminar entre sus usuarios en función del objetivo comercial o no del uso de esa página web. *«[S]i bien es cierto que también el titular de un sitio web goza de una serie de facultades para permitir y restringir el acceso al mismo, la singularidad de la red Internet hace que constituya*

9 Idem, p. 605, y los autores por él citados, entre ellos FERNÁNDEZ-ALBOR BALTAR, A.(2001). Régimen jurídico de la contratación en Internet. En GÓMEZ SEGADE (ed.), Comercio Electrónico en Internet, Madrid: Marcial Pons, pp. 239-240; y GUISADO MORENO, A. (2004), Formación y perfección del contrato en Internet, Madrid: Marcial Pons, pp. 184 y ss.

una contradicción el ofrecimiento público de facto sin restricciones y, al mismo tiempo, la pretensión de discriminar el acceso de los usuarios en atención a si son particulares o empresas que intervienen directamente, o si son agencias que intervienen por cuenta del particular o la empresa interesada en el vuelo».[10]

3. EL *SCREEN SCRAPING* DESDE LA ÓPTICA DE LA PROPIEDAD INTELECTUAL. APLICACIÓN DEL CONCEPTO DE BASE DE DATOS A PÁGINAS WEB Y POSIBLE INFRACCIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Otro de los puntos que reiteradamente son alegados en estos litigios es el relativo a la propiedad intelectual. El trasfondo jurídico del conflicto se centra en la existencia o no de una base de datos en el sitio web de *Ryanair* y en su protección por el derecho de autor por razón de la originalidad de su estructura –criterios de selección y de disposición–, y por el derecho *sui generis*, por haberse realizado una inversión sustancial por parte de *Ryanair* para la obtención, verificación o presentación de los contenidos de su página web, que habrían sido violados por las agencias de viajes al hacer uso no autorizado de la técnica del *screen scraping*.

Esta pretensión se ha venido denegando en las distintas instancias. En primera instancia se entiende que la página web de *Ryanair* cumple los requisitos para ser tenida por base de datos, pero no así las exigencias para poder quedar tutelada por alguno de los dos derechos de propiedad intelectual alegados por la actora. En segunda instancia, la Audiencia Provincial de Barcelona, en el asunto *Ryanair* contra *Edreams*, deja abierta la puerta a una doble alternativa: o bien considerar que no existía una base de datos, sino únicamente un programa de ordenador que genera los datos sobre la base de unos parámetros preestablecidos y que permite su consulta, o bien un programa de ordenador y una base de datos, pero esta última no habría de merecer la tutela del derecho de autor en su estructura, dado que también deriva del programa de ordenador. De entre estas dos posibilidades, la Audiencia Provincial se decanta por la primera. Entiende que lo que la página web de *Ryanair* contiene son los parámetros para calcular el precio (proximidad temporal del vuelo, número de plazas libres y criterios de política comercial), de forma que cada vez que se realiza una consulta el programa de ordenador genera un resultado sobre la base de estas reglas. No existe, por tanto, una recopilación de datos ori-

10 FJ 3º. Seguidamente, la Audiencia Provincial declara que la actora «está tratando de imponer una condición que no guarda relación directa con el acceso a la web, sino con la actividad económica o comercial que desarrolla alguno de sus usuarios» (…) «Dicho de otro modo, esa condición de uso no puede oponerse a la demandada, y en este sentido es irrelevante, pues excede propiamente del ámbito de control de la actora».

ginal en su estructura, ni tampoco una inversión sustancial en la obtención, verificación o presentación de datos preexistentes. La inversión se refiere a la creación o generación de esos datos, pues ha ido dirigida a la creación de un *software* que permite generar la información sobre la base de unos parámetros.[11]

El TS destaca que la existencia de una base de datos y su protección por el derecho de autor y/o por los derechos afines es una cuestión de hecho ajena a la casación, para, seguidamente, realizar un repaso por la jurisprudencia del Tribunal de Justicia de la Unión Europea recaída hasta la fecha en materia de bases de datos. La existencia de una base de datos está supeditada a la concurrencia de los siguientes requisitos: *«a) existencia de una recopilación de elementos independientes, separables unos de otros sin que resulte afectado el valor de su contenido informativo, literario, artístico, musical u otro; b) disposición sistemática o metódica de los elementos independientes recopilados; c) dotación de algún instrumento técnico, como pueden ser los procedimientos electrónicos, electromagnéticos o electroópticos, u otro instrumento, tal como un índice, sumario, plan o modo de clasificación que permita la localización de cualquier elemento independiente contenido en su seno –lo que la distingue de una colección de elementos que facilita información pero carece de todo instrumento de tratamiento de los elementos individuales que la componen–; y d) accesibilidad individual a los elementos recopilados»*.[12]

Asimismo, de manera ilustrativa y ciertamente acertada, el TS recalca que es la existencia de la base de datos lo que constituye el presupuesto para su protección por el derecho de autor y/o por el derecho *sui generis* como tal base de datos, y no a la inversa. En otros palabras, la existencia de una supuesta originalidad en la selección o disposición de los contenidos o una inversión sustancial en el tratamiento de esos contenidos resulta indiferente si no existe un continente y un contenido que cumplan con las exigencias de la definición europea de base de datos prevista en el art. 1.2 de la Directiva 96/9.

En lo que a la tutela por el derecho de autor se refiere, el TS hace un especial hincapié en la idea de que no se trata de una protección automática de toda base de datos. La originalidad únicamente se cumple cuando, mediante la selección o la disposición de los datos que contiene, su autor expresa su capacidad creativa de manera original tomando elecciones libres y creativas e imprime así su toque personal. Por el contrario, este criterio no se cumple cuando la constitución de la base de datos es dictada por con-

11 SAP de Barcelona de 17 de diciembre de 2009, FJ 4º. Para un estudio detallado de la problemática que conlleva la existencia de bases de datos complejas, necesitadas de un software para su efectivo funcionamiento, véase MINERO ALEJANDRE, G. (2014). La protección jurídica de las bases de datos en el ordenamiento europeo. Madrid: Tecnos, 215-218.

12 FJ 3º, apartado 45, en cita de la STJUE de 9 de noviembre de 2004, asunto Fixtures Marketing, C-444/02, apartados 29-32.

sideraciones técnicas, reglas o exigencias que no dejan espacio al ejercicio de la libertad creativa, como sucede en el litigio que nos ocupa.[13]

Más dudoso es si la base de datos puede ser protegida por la vía del derecho *sui generis*, que protege la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza el fabricante de una base de datos para la obtención, verificación o presentación de su contenido (art. 7.1 de la Directiva 96/9 y art. 133.1 LPI). El TS recuerda la doctrina *spin-off* aplicada por el Tribunal de Justicia de la Unión Europea: el derecho *sui generis* tutela la inversión sustancial en la obtención, verificación o presentación de sus contenidos, pero no así la inversión destinada a la creación *ex novo* de esos contenidos.[14] La falta de prueba en el caso concreto por parte de *Ryanair* de una inversión en su página web adicional a la destinada al *software* que permitía generar la información sobre los precios de sus vuelos conlleva la desestimación de la pretensión de tutela de *Ryanair*, dado que se entiende que los datos que se solicitan por las agencias en línea a través de la página web de *Ryanair* no preexistían, sino que eran creados por el *software* de titularidad de *Ryanair*.

CARBAJO CASCÓN se ha pronunciado de manera crítica sobre el contenido de la SAP de Barcelona que negaba la existencia de una base de datos. Este autor entiende que la amplitud del concepto de base de datos prevista en la Directiva 96/9 ha de servir para abarcar este tipo de productos.[15] Nosotros, sin embargo, entendemos que la reflexión es algo más compleja, pues supera los términos del examen sobre el cumplimiento o no del requisito de la independencia de los elementos, como criterio definitorio del concepto de base de datos, y se adentra en la división conceptual entre los términos base de datos y programa de ordenador a los efectos de su consideración como productos protegidos por la propiedad intelectual.[16] En efecto, las sentencias comentadas invitan a reflexionar

13 FJ 3º, apartado 47, en cita de la STJUE de 1 de marzo de 2012, Football Dataco Ltd y otros, C-604/10, apartados 29-39. Véase MINERO ALEJANDRE, G. (2012). Did the Database Directive actually Harmonise the Database Copyright) Football Dataco Lt. v. Brittens Pools Ltd. and the ECJ's Rules against Subsistence of Database Copyright in Fixtures Lists, European Intellectual Property Review, (10), 729-732.

14 FJ 3º, apartados 53-56, en cita de la STJUE de 9 de noviembre de 2004, asunto Fixtures Marketing, C-444/02, apartado 37.

15 CARBAJO CASCÓN, F. (2010). cit., 612.

16 El propio art. 1.3 de la Directiva 96/6 declara: «La protección prevista por la presente Directiva no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos». Ello se contrapone con el considerando 20º de esta norma europea, en el que se establece: «la protección prevista en la presente Directiva podrá aplicarse igualmente a los elementos necesarios para el funcionamiento o la consulta de algunas bases de datos como el Thesaurus y los sistemas de indización». El origen de esta contradicción deriva de la naturaleza de los índices y thesaurus habituales en bases de datos electrónicas: los programas de ordenador que los componen y permiten su funcionamiento.

sobre el origen de los elementos de una página web y a recordar que el examen de la existencia de un nivel de originalidad susceptible de tutela por el derecho de autor o una inversión sustancial para la protección de ésta por el derecho sui generis deben partir de este origen. De ello podemos inferir una total exclusión de este tipo de software con respecto de la protección de las base de datos. En primer lugar, porque la existencia de la base de datos debe examinarse con independencia de la existencia de un software que permita su uso, de manera que si, eliminado este segundo, la supuesta base de datos no pervive es porque la única realidad cuya protección jurídica habrá de valorarse es el programa de ordenador. En segundo lugar, porque si existiera una cierta estructura para el alojamiento y búsqueda de los elementos de la base de datos, adicional al programa de ordenador, pero los contenidos de la supuesta base de datos derivasen de un software que los genera de acuerdo con unas reglas previamente establecidas, la inversión en la creación y desarrollo de un programa de ordenador de este tipo –seguramente sustancial, dada su complejidad técnica– no podrá tenerse en cuenta a los efectos de la tutela sui generis de la base de datos, pues a esta inversión le será aplicable la jurisprudencia europea que ha excluido del cómputo de la inversión las partidas destinadas a la creación de los contenidos de la base de datos. En definitiva, si estamos al criterio finalista acogido por Tribunal de Justicia, un gasto que generalmente se califica como inversión a los efectos de su tutela sui generis, como es el desembolso necesario para la creación de un software que permite el funcionamiento de una base de datos, se excluye de dicho cómputo cuando el resultado de la aplicación del programa de ordenador a la base de datos no es ni la obtención, ni la verificación, ni la presentación de los datos de esa base de datos, sino su creación ex novo. En ambos casos, el titular de la página web cuyos contenidos han sido copiados mediante la técnica del screen scraping verá desechados sus alegatos sobre la existencia de un acto de extracción y reutilización sin su autorización, salvo que el código fuente del programa de ordenador haya sido reproducido –cosa que no interesará, generalmente, al supuesto infractor– y éste fuera original. En este último supuesto, el autor del código merecerá la protección por el derecho de autor sobre el software, pero no podrá controlar la extracción de datos.

Las sentencias estudiadas hasta ahora únicamente se refieren a los datos relativos al precio de los pasajes de avión, pero no así a informaciones sobre horarios y rutas, que no son generadas por el software conforme a los parámetros citados. Hubiera sido interesante que los tribunales que conocieron del litigio Ryanair v. Atrápalo se hubiesen pronunciado sobre la división conceptual entre programa de ordenador y base de datos que englobara todos los contenidos que realmente reproducía Atrápalo en su sitio web, y no únicamente los datos sobre el precio de los billetes. En este caso, seguramente, no hablaríamos de un único programa de ordenador, generador de la información sobre el precio, sino de varios. Concretamente, el software que genera los precios en función de las reglas preestablecidas, el programa de ordenador que ordena los resultados atendiendo a los parámetros sobre fechas, horarios, aeropuertos, precios, etc., elegidos por el

usuario, el programa que compila todas las reservas o compras que ha venido realizando un usuario y le permite su consulta, etc. Todos estos programas de ordenador se incluirán en la exclusión contenida en el art. 1.3 de la Directiva de bases de datos, pero el coste que supuso para el titular de la página web la creación o licencia de uso de todos y cada uno de estos programas de ordenador no tendrá que excluirse per se del cómputo de la inversión que pueda quedar protegida por el derecho sui generis, pues, a diferencia de lo que sucedía con el software al que se refiere la sentencia que se comenta, la función de estos otros programas de ordenador no es únicamente la creación o generación de datos, sino también su tratamiento.

De atenderse a este último tipo de datos y a este último tipo de programas de ordenador citados sí tendría sentido plantearse el examen del carácter sustancial o no de la inversión realizada en la creación y mantenimiento de ese software y el estudio del carácter sustancial o no de los datos empleados por las agencias de viajes on-line, a los efectos de concluir si el uso que éstas han realizado de los contenidos de la página web de Ryanair puede calificarse o no como extracciones y reutilizaciones que Ryanair pueda perseguir. En este último punto se debe tener en cuenta la posibilidad de análisis acumulativo previsto tanto en el art. 7.2 de la Directiva 96/9 como en el art. 133.3 LPI, que asimila el uso de la totalidad o una parte sustancial del contenido de una base de datos al uso repetido y sistemático de contenidos que si bien individualmente no serán suficientemente sustanciales, evaluados en su conjunto, por acumulación, sí lo son. Dicho carácter sustancial por acumulación habrá de determinarse ateniendo a la incidencia negativa que la extracción y/o reutilización repetida o sistemática de esos datos aislados pueda tener para la explotación normal de la base de datos y para los intereses del titular del derecho sui generis. Pues bien, parece complicado defender que, en las circunstancias del caso concreto, el comportamiento llevado a cabo por las agencias de viajes on-line mediante la técnica del screen scraping tenga por efecto impedir la explotación normal de la página web de Ryanair o perjudicar sustancialmente los intereses de la compañía aérea. Más bien parece que puede concluirse lo contrario, lo que conllevaría la no inclusión del comportamiento de las agencias de viajes on-line dentro del ámbito de control de Ryanair como potencial titular de un derecho sui generis sobre la inversión empleada en su página web.

Como continuación de lo anterior, para seguir alimentando la reflexión sobre este tipo de bases de datos complejas, no podemos terminar este apartado sin hacer mención de la STJUE de 19 de diciembre de 2013, C-202/12, asunto Innoweb contra Wegener, dado el parecido del supuesto de hecho con el que dio origen al litigio que nos ocupa. En este caso, el demandante, Wegener, proporciona acceso a través de su sitio web a una recopilación de anuncios de venta de vehículos, diariamente actualizada, compuesta por cerca de 200.000 vehículos. Aproximadamente 40.000 de esos anuncios se encuentran exclusivamente en este sitio web. Innoweb, demandado, ofrece un metamotor de búsqueda dedicado a la venta de vehículos, que utilizada los motores de búsqueda de otros

sitios de Internet, entre ellos, la página web de Wegener. En cada búsqueda Innoweb sólo muestra a sus usuarios una parte pequeña del contenido de la recopilación de Wegener, y ofrece hipervínculos a la página web de Wegener para que los usuarios puedan ampliar la información. La demanda de Wegener contra Innoweb, por infracción del derecho sui generis del primero sobre su sitio web, es estimada en lo esencial en primera instancia. El órgano de segunda instancia holandés, que conoce del recurso planteado por Innoweb, plantea cuestión prejudicial, con la que busca obtener una respuesta acerca de la calificación como infracción del derecho sui generis de actuaciones como las llevadas a cabo por el demandado en el asunto principal.

El Tribunal de Justicia contesta afirmativamente. Entiende que el art. 7.1 de la Directiva 96/9 debe interpretarse en el sentido de que «un operador que pone en línea en Internet un metamotor de búsqueda dedicado como el controvertido en el litigio principal está reutilizando la totalidad o una parte sustancial del contenido de una base de datos protegida por el citado artículo 7, puesto que dicho motor dedicado: proporciona al usuario final un formulario de búsqueda que ofrece, esencialmente, las mismas funcionalidades que el formulario de la base de datos; traduce en tiempo real las órdenes de búsqueda de los usuarios finales al motor de búsqueda del que está equipado la base de datos, de modo que se explotan todos los datos de dicha base; presenta al usuario final los resultados encontrados con la apariencia exterior de su sitio de Internet, agrupando las duplicaciones en un solo elemento, pero siguiendo un orden basado en criterios comparable a los empleados por el motor de búsqueda de la base de daos de que se trate para presentar los resultados».[17] El Tribunal de Justicia tiene en cuenta las características propias de un metamotor de búsqueda dedicado como el controvertido en el litigio principal –comunes a las características de los metamotores presentes en los litigios en los que ha sido parte Ryanair–, que no dispone de un motor de búsqueda propio que recorra los demás sitios de Internet, sino que se sirve de los motores de búsqueda de los que están equipadas las páginas web cubiertas por su servicio.[18] La utilización llevada a cabo por el metamotor afecta a una parte sustancial del contenido de la base de datos de que se trate, incluso a su totalidad, dado que un metamotor de este tipo «permite explorar todo el contenido de dicha base de datos, a semejanza de una orden de búsqueda introducida directamente en el motor de búsqueda de dicha base de datos. En estas circunstancias, carece de relevancia el número de resultados efectivamente encontrados y mostrador por cada orden de búsqueda introducida en el metamotor de búsqueda».[19] «Esta actividad de la persona que explota un metamotor de búsqueda dedicado como el

17 Apartado 54 y fallo.

18 Páginas web a las que el Tribunal de Justicia no duda en calificar como «bases de datos» a lo largo de la sentencia.

19 Idem, apartado 53.

controvertido en el litigio principal puede hacer perder dinero al fabricante de la base de datos, en particular el obtenido a través de la publicidad realizada en su sitio de Internet, privándolo de este modo de ingresos que se supone deberían permitirles amortizar el coste de su inversión en la constitución y funcionamiento de la base de datos».[20] Además, esta conclusión no varía por el hecho de que para acceder a toda la información sobre un resultado encontrado en una de las páginas web es necesario seguir el hipervínculo hacia esa página web de origen que figurará en la lista de resultados que se obtenga por el metamotor, pues muchos usuarios no verán ya la necesidad de hacerlo.[21]

4. EL *SCREEN SCRAPING* DESDE LA ÓPTICA DEL DERECHO DE LA COMPETENCIA DESLEAL

Finalmente, como recurso supletorio o subsidiario, *Ryanair* invoca en sus demandas y recursos la comisión de varios ilícitos por competencia desleal. De nuevo, esta pretensión es desestimada en todas las instancias, tanto en lo relativo al reproche de la infracción del art. 5 de la Ley de Competencia Desleal como en lo que se refiere a las infracciones de los arts. 11.2 y 12 de este cuerpo legal. En realidad, en su recurso de casación, tras las desestimaciones previas, *Ryanair* únicamente mantiene el fundamento de la vulneración de la cláusula general contenida en el art. 5 de esta ley, esto es, el aprovechamiento del esfuerzo ajeno, por entender que la extracción sistemática y puesta a disposición de los contenidos de su web mediante la técnica del *screen scraping* supone el aprovechamiento del sofisticado *software* que *Ryanair* tiene para generar los precios de sus vuelos y el cobro de un sobreprecio es un auténtico acto desleal de aprovechamiento indebido del esfuerzo competitivo de la recurrente por ofrecer billetes a los precios más económicos del mercado, sin intermediarios que sobrecarguen los precios, y que no repercutan en ganancias para *Ryanair*.

Se descarta que el comportamiento de las demandadas, consistente en hacer creer a sus clientes que las agencias de viajes gozan del consentimiento de *Ryanair* para vender sus billetes de avión, como intermediarias, encaje en los actos desleales por aprovechamiento de la reputación ajena regulados en el art. 12 de la Ley de Competencia Desleal, y ello porque no existe como tal un aprovechamiento. Las agencias de viajes actúan como meros agentes en la compra de billetes, pero no se presentan frente a sus clientes como agencias autorizadas por la compañía aérea, ni de tal manera que se asocien con

20 Idem, apartado 41. «[E]n particular porque a los operadores que deseen publicar anuncios publicitarios en línea les resultará más rentable hacerlo en el sitio de Internet del metamotor de búsqueda dedicado que en una de las bases de datos cubiertas por dicho metamotor» (apartado 42).

21 Idem, apartados 44-45.

el supuesto prestigio de *Ryanair*. Precisamente de lo que hay prueba es de lo contrario, pues *Edreams* y *Atrápalo* no se presentan formalmente bajo ninguna apariencia de relación o vinculación con *Ryanair*, entre otras razones porque esta última también denuncia que, al mostrar las agencias de viajes los resultados de las búsquedas solicitadas por sus clientes, si alguno de los vuelos ofertados es de *Ryanair*, se omite la referencia a dicha procedencia. Además, respecto al reproche del traslado a los clientes de las agencias *on-line* de la creencia generalizada de que esas agencias tienen autorización expresa o tácita de *Ryanair* para venderlos se señala que ha quedado constatado que el billete no lo emiten las agencias, sino *Ryanair*, de lo que es plenamente consciente el usuario, pues además del cargo del billete a favor de *Ryanair*, el cliente recibe otro cargo complementario correspondiente a la gestión por él solicitada a la agencia de viajes.

Asimismo, se deniega la subsunción de los hechos en la conducta tipificada en el art. 11.2 de la Ley de Competencia Desleal, pues falta el acto mismo de la imitación, esto es, crear una prestación a semejanza o ejemplo de otra de distinto empresario.

Finalmente, respecto al reproche de deslealtad por aprovechamiento del esfuerzo ajeno a través de la cláusula general de competencia desleal del art. 5 de la Ley de Competencia Desleal, sobre la que *Ryanair* insiste en casación, debe destacarse la conclusión alcanzada en segunda instancia, en la que se declara que la conducta de las agencias de viajes en línea no sólo no es contraria al derecho de la competencia, sino que fomenta dicho juego concurrencial. Se sostiene, citando la doctrina del TS, que la buena fe en sentido objetivo debe entenderse como la exigencia ética significada por los valores de honradez, lealtad, el justo reparto de la propia responsabilidad y el atenerse a las consecuencias que todo acto consciente y libre puede provocar en el ámbito de la confianza ajena.[22] Pero esta atención a los límites éticos de carácter general ha de entenderse subordinada a las exigencias directamente derivadas del principio de competencia económica, pues no debe reprimirse por el mero apoyo de límites éticos una conducta que se revele concurrencialmente eficiente, que promueva las prestaciones de quien la ejecuta o de un tercero por sus méritos, sin provocar una alteración en la estructura competitiva o en el normal funcionamiento del mercado.[23]

Eso es lo que ocurre en este caso, en donde las agencias de viaje, al prestar su servicio, no alteran la estructura competitiva ni el normal funcionamiento del mercado. En primer lugar, el uso que las agencias de viajes hacen del *software* de *Ryanair* no es distinto del que haría cualquier particular al solicitar directamente información sobre vuelos. En segundo lugar, esta conducta fomenta la competencia, pues permite al consumidor poder comparar distintas ofertas de vuelos que se acomodan mejor o peor a sus intereses, de tal forma que

22 SAP FJ 7º, en cita de las SSTS de 20 de marzo de 1996, 15 de abril de 1998, 16 de junio de 2000, 19 de abril de 2002 y 14 de marzo de 2007.

23 SAP FJ 7º, en cita de la STS de 8 de octubre de 2007.

quien acude a la agencia de viajes en línea lo hace para beneficiarse de esta información comparativa. Además, el negocio desarrollado por las agencias de viajes *on-line* no impide que los usuarios de Internet, tras identificar el vuelo que mejor se acomoda a sus intereses en la página web de la agencia en línea, decidan contratarlo directamente a través de la página web de la concreta compañía aérea que prestará el servicio de transporte. Ello es posible también en el caso de vuelos de *Ryanair*, pues los resultados de éstos aparecen identificados en la página web de la agencia en línea como vuelos de «compañía *low cost*». Incluso cuando el usuario decide contratar a través de la página web de la agencia en línea, el precio del billete es el fijado por *Ryanair* y es pagado directamente a la aerolínea, luego el modelo de negocio de ésta no se ve significativamente afectado, más allá de la pérdida de visitantes de la página web de *Ryanair* a los que esta última no va a poder ya ofrecer otros servicios adicionales que pueden contratarse desde su página web.

Con todo ello se afirma el carácter procompetitivo de la práctica de las agencias de viajes que utilizan el *screen scraping* en su labor de intermediación en la compra del billete y se recalca que las consecuencias de la conducta llevada a cabo por las agencias demandadas son consecuencias de la libre competencia del mercado, que *Ryanair* y el resto de operadores han de asumir desde que entran en ese juego concurrencial. En definitiva, si tras la ponderación de los intereses en juego se concluye que un concreto comportamiento resulta favorable para el desarrollo de la libre competencia en el mercado éste no podrá reputarse desleal, por molesto que pueda ser para alguno de los operadores.

6. BIBLIOGRAFÍA

Carbajo Cascón, F. (2010). Screen scraping o la extracción de datos de sitios web de terceros con fines comerciales. El conflicto entre Ryanair y las agencias de viajes en línea. (Comentario a la sentencia de la Audiencia Provincial de Barcelona, sección 15ª, de 17 de diciembre de 2009), *Actas de Derecho Industrial y de Derecho de Autor, 30,* 599-620.

Fernández-Albor Baltar, A.(2001). Régimen jurídico de la contratación en Internet. En Gómez Segade (ed.), *Comercio Electrónico en Internet,* Madrid: Marcial Pons.

García Vidal, A. (2013). Problemas jurídicos derivados del uso del screen scraping, Sentencia (Sala de lo Civil, Sección 1ª) núm. 572/2012, de 9 de octubre, *Cuadernos Civitas de Jurisprudencia Civil, 92,* 329-349.

Gómez Lozano, M.M. (2010). Vuelos de bajo coste, agencias de viajes virtuales y derecho de la competencia, *Revista de Derecho UNED,* 7, 599-615.

Guisado Moreno, A. (2004), *Formación y perfección del contrato en Internet,* Madrid: Marcial Pons.

Jennings, F., y Yates, J. (2009). Scrapping over data: are the data scrapers' days numbered?, *Journal of Intellectual Property Law & Practice, 4*(2), 120-129.

Minero Alejandre, G. (2014). La protección jurídica de las bases de datos en el ordenamiento europeo. Madrid: Tecnos.

Paniza Fullana, A. (2013). Una complicada relación a tres bandas: compañías aéreas low cost, agencias de viajes on line y consumidores, *Revista Doctrinal Aranzadi Civil-Mercantil, 11,* 41-50.

COMUNICACIONES SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS

DERECHO DE AUTODETERMINACIÓN INFORMATIVA Y EL DERECHO AL OLVIDO: LA GENERACIÓN «GOOGLE» DEL DERECHO A LA VIDA PRIVADA

Ana Azurmendi
Profesora de Derecho de la comunicación
Universidad de Navarra

RESUMEN: La comunicación que se presenta aborda el derecho de autodeterminación informativa y el derecho al olvido, en el contexto de la discusión del borrador del Reglamento europeo de Protección de Datos Personales, cuya aprobación está prevista para los próximos meses de 2014. El derecho al olvido ha cobrado fuerza argumentativa sobre todo a partir de algunos casos europeos que se consideran en el estudio. Los precedentes de este derecho así como la batalla frente a Google por parte de las agencias de protección de datos europeas ponen de manifiesto la diferente perspectiva adoptada sobre este problema, en Europa y en Estados Unidos. Si aquí se priorizaría el potencial del almacenamiento de datos personales para el desarrollo del marketing, del comercio electrónico y de la comunicación política –entre otros sectores–, Europa parece priorizar la libertad individual como clave del sistema democrático y los beneficios de los derechos a la vida privada y a la reputación.

Pero lejos de tratarse de un problema doctrinal o jurisprudencial que pueda resolverse mediante fórmulas legales o definiciones, es una realidad que afecta a millones de personas de todo el mundo, para quienes la tecnología ha ofrecido ya algunas soluciones, con aplicaciones que harían fácil tanto el control del usuario sobre sus datos como su borrado. Las conclusiones se centran en la necesidad de una regulación europea del derecho al olvido, tal y como plantea el borrador del nuevo Reglamento europeo, y en el horizonte tecnológico de una solución efectiva al problema de la difusión universal de datos personales.

PALABRAS CLAVE: Derecho al olvido, Autodeterminación informativa, Google, *Digital Ephemerality*.

1. LAS INICIATIVAS EUROPEAS Y ESTADOUNIDENSE PARA LA PROTECCIÓN DE DATOS PERSONALES: DIFERENTES PERSPECTIVAS Y EXTENSIÓN DE LA PROTECCIÓN

En enero de 2012, la Comisión Europea hizo público el borrador de un Reglamento de «Protección de Datos personales»[1] que vendría a sustituir a la Directiva 95/46/

1 En la actualidad su versión consolidada es de octubre de 2013, que es la que se maneja en la comunicación, accesible en http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf, con acceso 5 de febrero 2014. Borrador de enero

EC sobre la misma materia. Una de las principales novedades que presenta el borrador es el reconocimiento del derecho al olvido, definido como «el derecho de obtener del controlador[2] de un determinado dato personal su cancelación o eliminación y la abstención por parte del mismo controlador de diseminarlo». Esta iniciativa europea no es un acto aislado. En Francia se ha reconocido hace años un «*droit à l'oubli*» –es cierto que con referencia no sólo a datos personales, sino también a información sobre la vida privada que manejan los medios de comunicación– (Jeffrey Rosen, 2012: p. 88). En Alemania, a partir de la sentencia del Tribunal Constitucional de 1984, sobre el Censo de 1983, existe el «derecho de autodeterminación informativa» («*Recht auf Informationelle Selbstbestimmung*»)[3]. Y en España se reconocen ambos derechos: un derecho equivalente al derecho al olvido con la Ley Orgánica 15/1999, de «Protección de Datos Personales»(Artemi Rallo Lombarte, 2010: p.2), con el derecho de rectificación y cancelación de datos personales (art. 16); y, un derecho de autodeterminación informativa a partir de la Sentencia Constitucional de STC 292/2000, de 30 de noviembre[4].

Estados Unidos, ese mismo año 2012, publicó la «*Consumer Privacy Bill of Rights*» cuyo objeto era el mayor acceso y control de los consumidores sobre sus datos personales procesados por segundas y terceras partes. Pero, como el mismo nombre de la ley revela, las iniciativas europea y estadounidense no son del todo equiparables (Steven C. Bennet, 2012: p.168-171). En el caso de Estados Unidos la ley protegería sólo algunos datos perso-

---

de 2012 en *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* COM (2012) 11 final (Jan. 25, 2012), *accesible en* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf con acceso 5 de febrero de 2014.

2 El «Controlador» en definición recogida en el art. 4 (5) del borrador del Reglamento europeo de Protección de Datos es: «(…) the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes*, conditions* and means of the processing of personal data; where the purposes*, conditions* and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law».

3 Gerrit Hornung y Christoph Schnabel, «Data protection in Germany I: The population census decision and the right to informational self-determination», Computer Law & Security Report, Vol.25, n 1, 2009, pp 84-88.

4 Sentencia del Tribunal Constitucional 222/2000, de 30 de noviembre:
«La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. (Fundamento jurídico 6).

nales –los referidos a la privacidad– y obtenidos-procesados de sólo una parte de los usuarios: los consumidores. Mientras que las iniciativas europeas abordan el problema de todas las informaciones referidas a una identidad personal –sean o no relativas a la vida privada–, obtenidos-procesados de cualquier usuario (Steven C. Bennett 2012: pp. 164 y 165).

Se trata en ambos casos de reaccionar ante la necesidad puesta de manifiesto por diez Agencias de Protección de Datos –Alemania, Canadá, España, Francia, Holanda, Irlanda, Israel, Italia, Nueva Zelanda y Reino Unido– en 2010, que señalaban al motor de búsqueda *Google*, mediante acusaciones judiciales y extrajudiciales, por vulnerar de forma sistemática los derechos de protección de datos de ciudadanos.

2. *GOOGLE:* EL FRENTE DE BATALLA POR LA PRIVACIDAD

Han sido sobre todo los servicios *Buzz* y *Streetview* de *Google* los que han propiciado la reacción de las Agencias de Protección de Datos. En 2010, *Buzz*, una red social, había hecho públicamente visibles, por defecto, todas las direcciones de contacto de sus usuarios. Mientras que *Streetview* –un servicio de fotografías en tiempo real de las calles de las ciudades–, había recopilado miles de datos personales de usuarios de *wifi* en el paso de los automóviles de *Google* por innumerables localidades europeas, canadienses y neozelandesas.

Ante las acusaciones judiciales y extrajudiciales de aquel momento, *Google* argumentó que el problema se había resuelto al implementar una mayor transparencia, tal y como anunció en su web corporativa, en la que hizo públicos sus nuevos principios de privacidad[5].

Pero la tormenta sobre Google viene de lejos. La actitud de sus directivos, sus respuestas slogan del tipo «somos responsables, todo lo hacemos para mejorar nuestros servicios a nuestros usuarios» repetidas a coro por cada representante de la compañía contrasta –al menos en el tono– con su defensa frente a las demandas judiciales de «soy global ergo alegal». Todo esto más las declaraciones del CEO de Google, Eric Smith, al Wall Street Journal en agosto de 2010[6], ha motivado que, aunque la corporación no sea la única empresa que con carácter internacional opera con los datos personales de sus usuarios, al final, el debate sobre las nuevas dimensiones del derecho a la vida privada y de protección de datos personales en la era Internet se haya centrado en Google. Eric Smith, en la entrevista del periódico económico titulada «Google and the Search for the Future. The Web icon's CEO on the mobile computing revolution, the future of newspapers, and privacy in the digital age» afirmaba:

5 Accesibles en http://www.google.com/policies/technologies/ con acceso 5 de febrero de 2014.

6 Accesible la entrevista completa en http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212, con acceso 5 de febrero de 2014.

> «I actually think most people don't want *Google* to answer their questions (….) They want *Google* to tell them what they should be doing next. (…) Because of the info *Google* has collected about you, we know roughly who you are, roughly what you care about, roughly who your friends are.
>
> (…)
>
> «The power of individual targeting –the technology will be so good it will be very hard for people to watch or consume something that has not in some sense been tailored for them.»(…)
>
> «I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time»
>
> Añade el periodista: «He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites».

Erick Smith fue relevado de su cargo en abril de 2011. Pero posiblemente puso sobre la mesa uno de los temas más preocupantes en el entorno redes sociales-Internet: el riesgo que supone para la libertad de los individuos el enorme poder de información acumulado por las empresas de Internet. Un poder que básicamente consiste, por un lado, en su capacidad de predecir los comportamientos de millones de personas –previo conocimiento, durante años, de sus intereses, de sus comunicaciones personales, de sus intercambios de opiniones, sus *sites* favoritos, sus acciones profesionales, sus compras online, sus fotografías, las que de otros han publicado de ellas, y miles de cuestiones más-. Y, por otro lado, en la generación de unas identidades digitales que acompañen de por vida a los ciudadanos, determinando en muchos casos decisiones de su entorno profesional, personal, etc. Éste es el horizonte protegible de las nuevas versiones del derecho a la privacidad (Omer Tene 2011: p. 21).

3. LOS PRIMEROS CASOS SOBRE EL DERECHO AL OLVIDO

Tal y como señala Alessandro Mantelero (2013: p. 229), el derecho al olvido podría considerarse incluido en el derecho estadounidense, entre las intromisiones ilegítimas en la vida privada, dentro de la acción «*public disclosure of private fact*»; los casos *Melvin v.Reid* (1931) y *Sidis v. F-R Publishing Co*. (1940) serían los representativos de este *tort*[7]. Pero, como es evidente por las fechas, no se trata del «derecho al olvido» en los términos que ahora se plantean, sino de un tipo clásico de intromisión ilegítima en la vida privada: la difusión de hechos ciertos con alguna –pero no determinante– relevancia pública que dañan la reputación u otros intereses de una persona.

7 Ver un resumen de los dos casos en Alessandro Mantelero, «The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'», Computer Law & Secrutiy Review, 29, 2013, pp.230 y 231.

Sí se refieren al «derecho al olvido» los primeros casos resueltos en Italia y en Francia por sus respectivas autoridades de protección de datos, *Autorità garante per la protezione dei dati personali y la Commission Nationale Informatique et Libertés* (CNIL), sobre la publicación de datos por la *Autorità garante della concorrenza e del mercato*, en 2004[8] y por *LEXEEK*, en 2011, y el planteado en España por el camping «*Els Alfacs*» (*Alfacs Vacances)* contra *Google España*, en 2010 (con sentencia desestimatoria de 23 de Febrero de 2012 del Juzgado de Primera Instancia de Amposta, Tarragona).

La *Autorità garante per la protezione dei dati personali* resolvió la demanda planteada por un anunciante sancionado por publicidad engañosa por la agencia italiana de la competencia, *Autorità garante della concorrenza e del mercato*. Aquél había visto cómo su nombre aparecía en el boletín de la agencia de la competencia asociado al ilícito de publicidad engañosa. Como consecuencia de su difusión permanente en Internet, favorecida por los motores de búsqueda, se le estaba causando un grave perjuicio. El demandante no impugnaba la publicación en el boletín de la autoridad de la competencia, sino su «difusión en Internet sin adoptar las oportunas cautelas» (tales como el oscurecimiento de los nombres, o la posibilidad de permitir el acceso a las medidas sólo mediante una investigación dentro del sitio, donde los motores de búsqueda no pudieran acceder). Por el contrario, la autoridad de la competencia italiana estimaba que era necesario publicar la identidad del anunciante, puesto que «su omisión frustraría el propósito mismo de la legislación de la publicidad engañosa, especialmente cuando, como en este caso, de no tener esos datos, no sería posible identificar el anuncio». La *Autorità garante per la protezione dei dati personali* argumentó que la autoridad de la competencia podría seguir publicando sus medidas en su sitio web, pero «modulando el tiempo en el cual las decisiones relativas a las denuncias serán directamente detectables en Internet a través de los motores de búsqueda externos». Obligó a la autoridad de la competencia a incluir una sección dentro de su sitio web donde se puedan consultar por vía telemática aquellas decisiones con determinada antigüedad, y donde no sea posible la «directa detectabilidad de las decisiones contenidas en ella a través de motores de búsqueda externos». Al mismo tiempo, solicitó a la autoridad de la competencia que definiera el periodo de tiempo considerado proporcional para las finalidades perseguidas por la publicación de datos en su web.

En el caso francés, la CNIL publicó una resolución sancionadora en 2011 contra la asociación *LEXEEK*[9], que elabora bases de datos de sentencias judiciales publicadas

8 Caso comentado por Pere Simon Castellano en Pere Simon Castellano, «El derecho al olvido en el universo 2.0», Bid 28 (2012) DOI: 10.1344/105.000001808. http://bid.ub.edu/28/simon2.htm con acceso 4 de marzo de 2014.

9 Decisión accesible en http://www.cnil.fr/fileadmin/documents/La_CNIL/decisions/D2011-238_LEXEEK.pdf, con acceso 6 de febrero de 2014.

en Francia, por no eliminar en ellas los nombres y direcciones de las partes y testigos de los juicios, a pesar de los requerimiento de la CNIL, desde 2008, para que lo hiciera. El fundamento para la sanción condenatoria (de 10.000€) fue la «practique attentatoire au respect de la vie privée des personnes et au droit à l'oubli numérique».

En cuanto al caso del camping *Les Alfacs* la empresa denunció en 2010 a *Google España* por no atender a sus solicitudes de no situar entre los primeros resultados de búsqueda la tragedia sucedida en el camping en 1978; cuando la explosión de un camión cisterna cargado con propileno costó la vida de 243 personas. Se reclamaba el derecho al olvido y el derecho al honor de la empresa. Se pedía a *Google* que distinguiera las búsquedas sobre la tragedia de aquellas otras dirigidas a obtener información sobre el camping, puesto que la situación actual de presentación de resultados de búsqueda en *Google* perjudicaba de forma grave al negocio. El recurso fue desestimado porque la demanda debería haberse dirigido contra *Google.inc*, responsable de los contenidos y no contra *Google España*, responsable de la publicidad.

Sin duda *Autorità garante della concorrenza e del mercato, LEXEEK* y *Les Alfacs* ponen de manifiesto la necesidad de una protección específica más allá de la ofrecida por la tradicional «privacidad» o «derecho al honor». En los tres casos, una de las formas de resolver esa protección sería respetar una adecuada dosificación de los tiempos de publicación de la información. De manera que si bien es lógico, e incluso exigible, que un contenido informativo, perjudicial para los intereses de personas o empresas, sea accesible al conjunto de ciudadanos por circunstancias de su actualidad y relevancia, también es razonable que, una vez desaparecidas estas circunstancias, el perjuicio provocado por la publicidad pueda atenuarse. Bien mediante la inserción de los datos en una sección donde esos datos se hacen indetectables para los motores de búsqueda externos, bien mediante el anonimato de los protagonistas de los hechos ya juzgados o sancionados–utilizando iniciales en las decisiones o sentencias publicadas en Internet- o bien mediante la desvinculación en las búsquedas de las actividades actuales de personas físicas o jurídicas de los hechos noticiosos de hace décadas como ocurre en *Les Alfacs.* Un cuestión en la que profundiza Pere Simon Castellano (2, 2012: pp. 64-98).

4. LA RESPUESTA DEL ABOGADO GENERAL DEL TRIBUNAL DE JUSTICIA EUROPEO SOBRE UNA CONSULTA PREJUDICIAL SOBRE EL DERECHO AL OLVIDO

Existe un cuarto caso sobre derecho al olvido planteado por la AEPD frente a Google que ha originado una consulta de la Audiencia Nacional española al Tribunal de Justicia Europeo (Caso C-131/12) *Petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2012- Google Spain, S.L., Google, Inc. / Agencia*

de Protección de Datos (AEPD), Mario Costeja González[10]. En esta ocasión un ciudadano se ha visto perjudicado durante años por un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, publicado en el periódico La Vanguardia en 1998. Desde el momento en el que este medio de comunicación digitalizó todos sus números en papel, el nombre de Mario Costeja aparece vinculado, en las búsquedas de Google, a datos de su situación civil y patrimonial que son incorrectos en la actualidad. De esta situación se ha derivado un daño en su vida profesional. Solicitó primeramente a la Agencia Española de Protección de Datos que se exigiera al periódico la eliminación de esos datos pero la petición no prosperó. La Agencia estimó que la publicidad de la subasta realizada en La Vanguardia era legal. Su eliminación significaría atentar contra la libertad de expresión. Sin embargo, la AEPD solicitó a *Google España* y *Google Inc.* que dejara de indexar este contenido. *Google* recurrió la acción de la Agencia –junto con otras más semejantes– ante la Audiencia Nacional.

Este órgano jurisdiccional elevó consulta prejudicial ante el Tribunal de Justicia Europeo en 2012, con el objeto de obtener aclaración sobre aspectos concretos de la Directiva 95/45/EC de «Protección de Datos Personales» y, así, perfilar mejor su aplicabilidad a determinadas acciones del motor de búsqueda *Google*. Junto a esto, pretendía precisar los argumentos para poder exigir a la empresa de Internet acciones relacionadas con la garantía del derecho al olvido. Entre otras se hacía la pregunta:

> «3.1. ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulados en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?»

El preámbulo de la decisión prejudicial llegó el 25 de junio de 2013, con las Conclusiones del Abogado General del Tribunal de Justicia Europeo Niilo Jääskinen[11], que se resumirían en:

a) Los proveedores de servicios de motor de búsqueda en Internet no son responsables, sobre la base de la Directiva sobre Protección de Datos, de los datos personales incluidos en las páginas web que tratan.

---

10 Se trata de la *Petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2012- Google Spain, S.L., Google, Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González* accesible en http://curia.europa.eu/juris/document/document.jsf?docid=123131&doclang=ES, con acceso 11 de febrero de 2014.

11 Conclusiones accesibles en http://curia.europa.eu/juris/document/document.jsf?text&docid=138782&pageIndex=0&doclang=ES&mode=req&dir&occ=first&part=1&cid=362663 con acceso 11 de febrero de 2014.

b) La normativa nacional de protección de datos les es de aplicación (a los proveedores de servicios) cuando establecen en un Estado miembro una oficina que orienta su actividad hacia los habitantes de dicho Estado. Aunque el fin de esta oficina sea el de promover y vender espacios publicitarios en su motor de búsqueda y aunque el tratamiento técnico de los datos se realice en otro Estado, sea o no miembro de la Unión Europea.

c) Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido.

En la exhaustiva línea argumental del Abogado General, señalaba entre otras cuestiones:

«B. *Motores de búsqueda en Internet y protección de datos*

32. Al analizar la posición legal de un motor de búsqueda en Internet en relación con las normas de protección de datos, deben tenerse en cuenta los siguientes elementos.

34. (…), los resultados que ofrece un motor de búsqueda en Internet no se basan en una búsqueda instantánea de todo el World Wide Web, sino que se compilan a partir del contenido que el motor de búsqueda en Internet ha tratado previamente. Ello significa que el motor de búsqueda en Internet ha recopilado contenidos a partir de páginas web existentes y que ha copiado, analizado e indexado dicho contenido en sus propios dispositivos. Este contenido recuperado contiene datos personales si éstos figuran en alguna de las páginas web fuente.

35. (…) para que los resultados sean más fáciles de usar, los motores de búsqueda normalmente muestran contenidos adicionales además del enlace a las páginas web originales. Pueden ser extractos de texto, contenido audiovisual o incluso instantáneas de las páginas web fuente. Esta vista previa de la información puede, al menos en parte, recuperarse a partir de los dispositivos del proveedor de servicios de motor de búsqueda en Internet, y no instantáneamente desde la página web original. Ello quiere decir que el proveedor del servicio está realmente en posesión de la información expuesta de este modo.»

Y continúa en su aclaración para la Audiencia Nacional española:

«D. *El papel y la responsabilidad de los editores de la página web fuente*

42. (…) técnicamente, el editor tiene la posibilidad de incluir en sus páginas web códigos de exclusión que restringen el indexado y el archivo de la página y que, por tanto, incrementan la protección de datos personales. En casos extremos, el editor puede retirar la página web del servidor de alojamiento, volver a publicarla sin los datos personales controvertidos y solicitar que se actualice la página en las memorias ocultas de los motores de búsqueda.

44. No obstante, la responsabilidad del editor no garantiza que los problemas de protección de datos puedan abordarse de manera definitiva recurriendo sólo a los responsables del tratamiento de las páginas web fuente. (…)

> 45. De hecho, la accesibilidad universal de la información en Internet se basa en los motores de búsqueda en Internet, ya que sin ellos hallar información relevante sería demasiado complicado y difícil y produciría resultados limitados (…)

Acerca de lo que plantea *Google* para evadir la aplicación de la Directiva Europea, al señalar que es *Google.Inc* con sede en California la empresa que trata los contenidos y que *Google* España únicamente se dedica al negocio publicitario, se responde:

> «68. (…) se lleva a cabo tratamiento de datos personales en el marco de las actividades de un 'establecimiento' del responsable del tratamiento, en el sentido del artículo 4, apartado 1, letra a), de la Directiva, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, a fines de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado».

Y sobre el derecho al olvido:

> «109. Aunque el Tribunal de Justicia declarase que los proveedores de servicios de motor de búsqueda en Internet se responsabilizan, como responsables del tratamiento, *quod non,* de los datos personales contenidos en las páginas web fuente de terceros, un interesado tampoco tendría un 'derecho al olvido' absoluto que pudiera invocar frente a los proveedores de servicios. Sin embargo, el proveedor de servicios necesitaría ponerse en la posición del editor de la página web fuente y comprobar si la difusión de los datos personales en la página web podría considerarse legal y legítima a los efectos de la Directiva. Dicho de otro modo, el proveedor de servicios necesitaría abandonar su función de intermediario entre usuario y editor y asumir la responsabilidad por el contenido de la página web fuente y, cuando resultase necesario, censurar el contenido evitando o limitando el acceso a éste».

En definitiva: se asume y reconoce el «derecho al olvido» frente al proveedor de servicios, aunque con un matiz de subsidiariedad respecto al editor de la página web fuente, aspecto que no queda completamente aclarado en la respuesta ofrecida por el Abogado General.

5. TEMPORALIDAD DE LOS DATOS PERSONALES O DIGITAL EPHEMERALITY COMO UNA SOLUCIÓN VINCULADA AL DERECHO AL OLVIDO

En todos los casos mencionados, los datos personales sobre los que se solicita «derecho al olvido» habían tenido una difusión proporcionada a su relevancia en el momento de su primera publicación. Así, es lógico que una sanción a un anunciante por publicidad engañosa se publique en el boletín de la autoridad de la competencia (Caso Autorita garante de la concorrenza), como lo es que en una sentencia original aparezcan nombradas las partes que intervienen (caso *LEXEEK), que en un periódico se informe de un accidente de dimensiones catastróficas (caso «Els Alfacs») o que se dé publicidad a una subasta de bienes con carácter previo a su celebración (caso «Mario Costeja»). Sin embargo, el hecho de que, hasta 10 y 15 años después, esos mismos datos estén accesibles con carácter ilimitado a un número indeterminado de personas no parece tan lógico*

si ocasiona perjuicios notables, de tipo moral y económico, a las personas físicas o jurídicas nombradas, cuando las circunstancias que fueron la causa de aquella publicación ya no perduran en la actualidad.

Una de las soluciones que se barajan para mitigar este perjuicio, a la vez que se respeta la libertad de expresión, consiste en establecer un plazo de tiempo razonable para la accesibilidad universal de este tipo de datos, a partir del cual se deberían:

a) Eliminar esos datos de la fuente original, sustituyéndolos por iniciales (parece apropiado para las publicaciones de resoluciones y sentencias judiciales, en algunos casos también para periódicos).

b) Plantear un doble paso en el acceso a la información, de manera que los contenidos publicadas por medios de comunicación a partir de una fecha con respecto a su difusión inicial pasen a un fondo de hemeroteca que no sería accesible directamente para los motores de búsqueda, sino que sería necesario entrar en la web del medios de comunicación y desde ahí iniciar otro proceso de registro y de búsqueda para el acceso a los números anteriores a esa fecha.

Temporalidad de los datos frente a su permanencia en Internet es una de las ideas de las que más se habla como medio para incorporar el derecho al olvido (Susan Corbett 2013: p. 148). Otra solución cercana sería, en palabras de Meg Leta Ambrose (2013: p.1) la Digital Ephemerality. Se trata de una exigencia que podría vincularse al «derecho al olvido» sobre determinados datos, pero que, al mismo tiempo, es ya un objetivo buscado por muchos usuarios de Internet con el Snapchat –una aplicación de móvil que permite a los usuarios enviar fotos que desaparecen en 10 segundos– o por empresas como Reputation.com o Reputación en Internet, o Abine que vende el servicio DeleteMe que elimina perfiles públicos de las principales webs de datos, información social y de contacto, fotos personales etc. Abine, al mismo tiempo, oferta el servicio de lanzar los contenidos positivos sobre sus clientes a los primeros resultados de búsquedas. Tal posibilidad de control sobre los contenidos relativos a la propia persona muestra la proximidad del derecho al olvido con el derecho de autodeterminación informativa.

Hoy por hoy, cualquiera de estas soluciones parece difícil de aplicar en la práctica, a pesar de que hay investigaciones en marcha que muestran un futuro de mayor control de los ciudadanos sobre sus datos personales. Como el proyecto «Vanish»[12] de la Universidad de Washington, mencionado por Susan Corbett (2013: nota 64, p. 149), en el que se está trabajando sobre un sistema de encriptación cuya función sería la autodestrucción de los datos después de un periodo de tiempo determinado. Así, en lugar de confiar en que será Google, Facebook o Hotmail quienes eliminan los datos almacenados, será «Vanish» quien encripte los datos y luego deshaga la clave de encriptamiento.

12 Más sobre el proyecto en http://vanish.cs.washington.edu/ con acceso 28 febrero 2014.

Pero la oposición a esta temporalidad del mantenimiento de datos personales en Internet tiene también su razón de ser. El derecho a la información (David S. Ardia 2010: p. 30) o necesidades públicas como la seguridad (Jef Ausloos 2012: p. 149) quedan o, cuando menos, pueden quedar muy neutralizados ante un derecho al olvido que podría eliminar de forma definitiva informaciones importantes. Una de las críticas más repetidas contra el derecho al olvido es que, de aplicarse, se estaría facilitando un tipo de censura sutil, en la medida en que, si se permite a todas las personas eliminar sus datos personales según su deseo, dejarían de estar accesible datos relevantes y, en consecuencia, podría darse lugar a una falsificación de la realidad. Por esta razón, en opinión de Ardia y Ausloos, al constatar que, en muchas ocasiones, no es posible discernir qué información de la accesible en la actualidad será relevante en un futuro, sería preferible no considerar un derecho al olvido generalizado. Por otro lado, María Eduarda Gonçalves e Inés Andrade (2013: pp. 255-259) y Troncoso Reigada (2012: p.16) consideran que hay otras razones añadidas a las del derecho a la información, la libertad de expresión y a la necesidad de seguridad, como son:

a) razones de interés público en el área de salud pública;

b) finalidades de carácter histórico, estadístico y de investigación científica;

c) el cumplimiento de la obligación legal de conservar datos personales.

Unos límites que, desde su punto de vista, son muy difíciles de equilibrar con el derecho al olvido, hasta el punto de que la «metáfora de la proporcionalidad» en la ponderación de derechos en conflicto no funciona de forma correcta en el caso de los datos personales[13].

6. EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA

Las empresas Reputation.com o Reputación en Internet, o Abine no sólo son un negocio de eliminar datos personales, sino que, al mismo tiempo, ofrecen servicios de posicionamiento en los resultados de búsquedas acerca de sus clientes. Tal posibilidad de control sobre los datos relativos a la propia persona muestra la proximidad existente entre el derecho al olvido y el de autodeterminación informativa, un derecho de construcción jurisprudencial reconocido por primera vez en Alemania en la influyente sentencia del Tribunal Constitucional de 1983, recurso de amparo contra la Ley del «Censo de Población, Profesiones, Viviendas y Centros de Trabajo» de 1982[14]. Se definió entonces como:

13 Lorenzo Cotino Hueso (2011: pp. 396-399) hace una aportación sobre las posibles soluciones a estos conflictos entre derechos.

14 Han estudiado esta sentencia, entre otros, Gerrit Hornung y Christoph Schnabel, «Data protection in Germany I: The population census decision and the right to informational self-deter-

> «facultad del individuo para determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona»; un derecho al «libre desarrollo de la personalidad en las actuales condiciones de procesamiento de datos personales que implica la protección del individuo frente a una ilimitada recolección, archivo, uso y transmisión de sus datos personales»[15]

El derecho de autodeterminación informativa se comprende aquí como la prerrogativa individual sobre la publicación y uso de datos personales propios, que genera una obligación de protección frente a una recolección y tratamiento indiscriminado de los mismos. Este derecho no se fundamenta en el derecho a la vida privada, sino, principalmente,

> «en los valores de libertad y dignidad humana en relación con el desarrollo de la personalidad».

Según esta sentencia, el tratamiento automatizado de datos de carácter personal podía

> «repercutir en (la) libertad de decidir en la medida en que el individuo no sabe lo que los terceros conocen de él y en tanto en cuanto, siendo conocedores de información acerca de su persona, ellos sí pueden prever su decisión».

Es decir: el alto grado de predicción de las conductas y decisiones de los ciudadanos, que hoy es posible conseguir gracias al cruce de una cantidad inmensa de datos personales recabados en Internet, limitaría de forma considerable la libertad real existente en una sociedad. De este modo, se erosionaría el núcleo del sistema democrático, fundado sobre el reconocimiento de la libertad de los ciudadanos (cfr. Martínez Martínez, Ricardo, 2004: p. 242). El caso del técnico informático Edward Snowden, ha puesto sobre la mesa –entre otras cuestiones– la capacidad de la NSA (Agencia Americana de Seguridad) de recolectar datos personales de millones de usuarios de Internet a través del programa PRISM, mediante la entrada directa a los grandes proveedores de servicios de telecomunicaciones y de la red: *Yahoo, Google, Facebook, Youtube, Skype, AOL y Apple*[16].

En España, el Tribunal Constitucional reconoció por primera vez el derecho de autodeterminación informativa en la Sentencia 292/2000, en la que declaró inconstitucionales varios incisos de los artículos 21.1 y 24.1 y 2, de la Ley Orgánica 15/1999

---

mination», Computer Law & Security Report, Vol.25, n 1, 2009; Antonio Enrique Pérez Luño, «La defensa del ciudadano y la protección de datos», Revista Vasca de Administración Pública 14(1986) pp.43-55; David H., Flaherty, *Protection pirvacy in surveillance societies. The Federal Republic of Germany, Sweden, France, Canada and The United States* (2 ed., North Carolina Press, Chappel Hill 1992) pp. 46 y ss.; y Ricardo Martínez Martínez, *Una aproximación crítica a la autodeterminación informativa* (Thompson-Civitas, Madrid 2004) p. 241.

15 Traducción a partir de la que hace del original alemán Flaherty, op.cit.

16 Ver «The Guadian»6 junio 2013 en http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data con acceso 25 febrero 2014.

de «Protección de Datos Personales», considerando que vulneraban el derecho a la intimidad, ya que permitían las cesiones de datos entre Administraciones públicas para fines distintos a los que motivaron su recogida; y, además, en el momento de recabar los datos, no era necesario para la Administración informar al ciudadano de que esa cesión podía darse. Tal como señala la sentencia se trataría de un nuevo derecho fundamental de «autodeterminación informativa», de «libertad informática» (en atención a sentencias anteriores del mismo tribunal, como las STC 245/1993, de 20 de julio; 143/1994, de 4 de mayo; 11/1998, de 13 de enero; 94/1998 de 4 de mayo; y 202/1999, de 8 de noviembre) o simplemente «de protección de datos personales». Los casos que se habían presentado con anterioridad a éste –un recurso de inconstitucionalidad del Defensor del Pueblo por algunos incisos de artículos de la ley de 1999– habían ido desde la denegación de un Gobierno Civil –el de Guipúzcoa– a dar información a un ciudadano sobre los datos que poseía sobre su persona (STC 254/1993) a la negativa de una entidad de crédito a que un empleado cancelara sus datos médicos de un fichero informatizado de la empresa (STC 202/1999)[17].

Como señala el Tribunal Constitucional, la protección de datos personales es:

> «una forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los 'derechos de la persona'» (STC 292/2000, Fundamento jurídico 4), pero es «también, 'en sí mismo, un derecho o libertad fundamental'» (STC 292/2000, Fundamento jurídico, n. 4).

Es un derecho:

> que se diferencia del «derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar» (STC 292/2000, Fundamento jurídico 6).

La peculiaridad del derecho a la protección de datos consiste en su distinta función, que es garantizar a los individuos un poder de disposición sobre esos datos (cfr. STC 291/2000, Fundamento jurídico 6) y no tanto lo que caracteriza al derecho fundamental a la intimidad: «proteger frente a cualquier invasión que pueda realizarse en aquél ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad» (STC 292/2000, Fundamento jurídico 6).

Sin embargo, como apuntan Rapahel Gellert y Serge Gutwirth (2013: p. 522), no siempre funciona la distinción entre el derecho a la protección de datos y el derecho a la vida privada, puesto que, aunque la regulación europea –sobre todo la Directiva 94/46/EC de Protección de Datos y el borrador actual de 2013 del Reglamento de Protección

17 Estudia esta sentencia Concepción Conde Ortíz La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, Madrid, 2005 accesible en http://app.vlex.com/#/vid/291636 con acceso 5 marzo de 2014.

de Datos– así lo considere, el hecho de que el Convenio Europeo de Derechos Humanos sólo contenga en su artículo 8 la referencia al derecho a la vida privada, ha significado que el Tribunal Europeo de Derechos Humanos haya resuelto casos relativos a protección de datos bajo el paraguas del derecho a la vida privada.

7. DERECHO AL OLVIDO Y A LA AUTODETERMINACIÓN INFORMATIVA EN LA NUEVA PROPUESTA DE REGLAMENTO SOBRE DATOS PERSONALES

El derecho al olvido está incluído en el borrador del nuevo Reglamento de la Unión Europea de Protección de Datos Personales, norma que actualizará la Directiva europea de 1995. Su objetivo es lograr una mayor uniformidad en la protección de datos entre los Estados Miembros, algo que no se ha conseguido hasta el momento. Al contrario, se tiene la experiencia de la dificultad de aplicación armonizada de la Directiva 95/46/EC (Paul De Hert y Vagelis Papakonstantinou, 2012: p. 131). Otras de las finalidades del Reglamento propuesto son: una mejor protección frente a amenazas que no existían en los años 90 y el incremento de la vigilancia sobre los controladores de datos no europeos (Meg Leta Ambrosse, 2013: p. 9).

Entre la versión del borrador, aprobada por la Comisión Europea en enero de 2012, y la versión consolidada de octubre de 2013, el derecho al olvido ha sufrido un rebajamiento considerable de su intensidad garantista, hasta el punto de desaparecer incluso del título del artículo 17. El escepticismo que había suscitado la formulación inicial, así como las críticas acerca del reconocimiento del derecho de obtener el borrado sobre datos transferidos a terceras partes o que se habían autorizado transferir a terceras partes han tenido su efecto. En apariencia, con la nueva redacción de octubre de 2013, se equilibraría mejor el derecho al olvido con otros derechos humanos. Yendo al análisis del texto:

El artículo 17, «Right to erasure», contempla, en primer lugar, el derecho de cada persona a obtener del controlador de datos el borrado de sus datos personales, de forma inmediata, cuando,

- no sean ya necesarios para el propósito para el que fueron recogidos y tratados;
- el sujeto de los datos retire el consentimiento;
- un tribunal o autoridad reguladora establecidos en Europa determine de forma definitiva que el dato debe ser borrado; o
- que el dato ha sido procesado ilícitamente.

Sólo en casos excepcionales se permitirá al controlador retener y no borrar los datos:

a) Para la defensa del derecho a la libertad de expresión de acuerdo con el art. 80;
b) Por razones de interés público en el área de salud pública, de acuerdo con el art. 81;

c) Para finalidades de investigación histórica, estadística y científica, de acuerdo con el art. 83(el cual, en cualquier caso, requiere que cualquier dato personal se conserve de forma separa del resto de información bajo los más altos estándares técnicos);

d) Por cumplimiento de obligación legal de conservación;

e) Cuando la retención de datos personales es necesaria para el cumplimiento de un contrato;

f) Los datos deben mantenerse con finalidades de prueba; o

g) El tipo particular de tecnología de almacenamiento no permite la eliminación y haya sido instalado con anterioridad a que el Reglamento entre en vigor.

En el caso de f y g, el controlador de datos debe restringir el procesamiento de los datos personales, de manera que los datos retenidos no están sujetos al acceso y a las operaciones de procesamiento normales, sino sólo retenidos para finalidades específicas.

Constituirían facultades del derecho al olvido, aunque no se menciona en el texto como tal, la obligación de borrado inmediato de datos personales de los servidores en internet del controlador, foros, comunidades, plataformas, etc. Sin embargo, se ha eliminado la obligación general de dar los pasos razonables para informar a terceras partes que procesen datos publicados (sería el caso de motores de búsqueda a quienes se permite rastrear redes sociales) acerca de su obligación de eliminar links, copias o replicaciones de datos personales. Sólo cuando no hay justificación legal para la publicación de datos permanece la obligación de informar (por ejemplo si no hay consentimiento para la publicación de los datos). Con todo, esta fórmula contenida en la versión consolidada del borrador del Reglamento es un reconocimiento del derecho al olvido. El hecho de que se evite darle este nombre es más una cesión a las acciones de lobby de las grandes empresas estadounidense de Internet que un cambio sustancial en la política de la Comisión Europea al respecto.

8. CONCLUSIONES

El derecho al olvido europeo se plantea como un conjunto de posibilidades de acción de los ciudadanos para eliminar sus datos personales en Internet siempre que se cumplan una serie de condiciones establecidas por ley. Tales facultades quedarían aún por delimitar pero estarían centradas en la facultad de borrar los datos, aunque contemplarían otras como la facultad de obtener del controlador de datos la abstención de continuar con su diseminación, así como de obtener de terceras partes el borrado de cualquier enlace a los mismos, o copia o replicación de tales datos, tal y como contempla el art. 17 del borrador del nuevo Reglamento de protección de datos. Su objeto es garantizar un marco de libertad para el individuo en la vida social en unas circunstancias, como las de la Sociedad de la Información, en la que existe, por una parte, un alto grado de predicción de conductas y decisiones de los ciudadanos y, por otra, una accesibilidad

universal a datos personales, precisamente por la inmensa capacidad existente de recolección, tratamiento y difusión de datos. La temporalidad sería una de las claves para preservar el derecho, de forma que la accesibilidad de datos en función de plazos determinara una cierta proporcionalidad con respecto a la limitación de otros derechos en juego, como el derecho a la información. Pero junto al establecimiento de unos tiempos y la articulación de unas posibilidades de acción, el horizonte del derecho al olvido debe de tener en cuenta también soluciones tecnológicas. En la actualidad, las iniciativas englobadas en la Digital Ephemerality facilitan tanto la desaparición de perfiles personales de Internet como el diseño de la propia identidad digital.

9. BIBLIOGRAFÍA

Ardia, D. (2010), Reputation in a Networked World: Revisiting the Social foundations of Defamation Law. *Havard Law Review,*

Ausloos, J. (2012),The Right to be Forgotten, a Worth remembering? *Computer Law & Security Review, 28.*

Bennett, S. (2012) The 'Right to Be Forgotten': Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, 30, (1).

Conde Ortíz, C. (2005) *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid: Dykinson. Recuperado el 5 de marzo de 2014 en http://app.vlex.com/#/vid/291636

Corbett, S. (2013), The retention of personal information online: A call for international regulation of privacy law. *Computer Law & Security review* , 29.

Cotino Hueso,L. (2011) La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución en Cotino Hueso, L. (ed) *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenzas y garantías*, Valencia: Publicacions de la Universitat de València, pp.. 386-401.

De Hert, P., y Vagelis Papakonstantinou, V. (2012), The proposed data protection Regulation replacing Directive 95/46/EC, A sound system for the protection of individuals. *Computer law & Security review*, 28.

Flaherty, D.(1992) *Protection privacy in surveillance societies. The Federal Republic of Germany*, Sweden, France, Canada and The United States (2 ed.), Chappel Hill: North Carolina Press.

Gellert, R. y Gutwirht, S. (2013) The legal construction of privacy and data protection computer. *Computer Law & Security Review*, 29.

Gonçalves, M.E. y Andrade, I. (2013) Security policies and the weakining of personal data protection in the European Union. *Computer&Security review*, 29, pp. 255-263.

Hornung, G. y Christoph Schnabel, Ch. (2009) Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Report*, 25, (1).

Leta Ambrose, M. (2013) A digital Dark Age and the Right to be forgotten. *Journal of Intenet Law*, 17, (3).

Mantelero, A. (2013), The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Securty Review*, 29.

Martínez Martínez, R. (2004) *Una aproximación crítica a la autodeterminación informativa*, Madrid: Thomposon-Civitas.

Pérez Luño, A.E. (1986), La defensa del ciudadano y la protección de datos. *Revista Vasca de Administración Pública*, 14.

Artemi Rallo Lombarte, A. (2010) El derecho al olvido y su protección. A partir de la protección de datos. *Telos: Cuadernos de comunicación e innovación*, 85. Recuperado el 7 de marzo 2014 en http://telos.fundaciontelefonica.com/seccion=1268&idioma=es_ES&id=2010110416500001&activo=6.do

Jeffrey Rosen, J. (2012), The Right to be Forgotten. *Stanford Law Review online*, 64. Recuperado el 3 de marzo 2014 http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

Simon Castellano, P. (2012), *El régimen constitucional del derecho al olvido digital*. Valencia: Agencia Española de Protección de Datos y Tirant lo Blanch.

Simon Castellano, P. (2012), El derecho al olvido en el universo 2.0., *Bid* 28. DOI: 10.1344/105.000001808 Recuerpado el 4 de marzo 2014 en http://bid.ub.edu/28/simon2.htm

Tene, O. (2011), Privacy: the new generations. *International Data Privacy Law*, 1, (1).

Troncoso Reigada, A. (2012), El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea. *Revista de Derecho, comunicaciones y Nuevas Tecnologías*, 8.

Troncoso Reigada, A. (2013) Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. *Revista de Internet, Derecho y Política*, 16.

11

A NEW PARADIGM FOR DATA PROTECTION

Alessandro Mantelero
Aggregate Professor, Politecnico di Torino
Director of Privacy and Faculty Fellow, Nexa Center for Internet and Society

ABSTRACT: The complexity of data processing and the power of modern analytics drastically limit the awareness of data subjects, their capability to evaluate the various consequences of their choices and their free and informed consent.

Although some aspects –namely the data protection impact assessment and the privacy by design approach– concur in shifting the focus of the regulation from users' self-determination to security and risk assessment, notice and consent are still fundamental aspects of the new EU Proposal for a general data protection regulation. Nevertheless, the «transformative» use of personal data in the Big Data context often makes it impossible to give the description of all the possible uses of the data at the time of their initial collection.

To respond to the above, the paper reconsiders the historical evolution of data protection and the fundamental issues of the related regulations. The author suggests a revision of the «notice and consent» model focused on the opt-in, from the first generations of data protection regulations to the new EU proposal. The paper proposes the adoption of a different approach when, such as in Big Data collection, the data subject cannot be totally aware of the tools of analysis and their potential output.

For this reason, the author sustains the provision of a subset of rules for Big Data analyses, which is based on the different opt-out model and on a deeper level of control by data protection authorities.

KEYWORDS: Data protection reform, notice and consent, opt-in model, Big Data, data protection authorities.

1. INTRODUCTION

In the last few years, the debate surrounding data protection and privacy has focused on the future wave of new regulations. Driven by the Web 2.0 environment and the economy of data, private companies and governments have become even more data-centric. However, the high demand for personal information, the complexity of the new tools of analysis and the increasing numbers of sources of data collection, have generated an environment in which the «data barons»[1] (i.e. big companies, government agencies,

1 See Mayer-Schönberger, V., Cukier, K. (2013). Big Data. A revolution That Will Transform How We Live, Work and Think (p. 182). London: Jhon Murray.

intermediaries)[2] have a control over digital information which is no longer counterbalanced by the user's self-determination. Nevertheless, all the ongoing proposals for a reform of data protection regulations, both in the U.S. and Europe, are still focused on the traditional main pillars of the so called «fourth generation» of data protection laws[3], which are represented by the purpose specification principle, use limitation principle and the «notice and choice» model[4]. This kind of approach seems to be inadequate in the present Big Data context and in a digital world characterized by an asymmetric distribution of the control over information. It is also inadequate in a digital economy where users accept not having an effective negotiation of their personal information, due to market concentration and social and technological lock-ins.[5]

For these reasons, it is necessary to re-consider the existing data protection legal framework and define new models, which better address the various issues of this new digital environment. Different proposals have been advanced by legal scholars, which focus on privacy by design[6], contextual privacy[7], data uses[8] and other combined solutions. Nevertheless, many of these proposals adopt a holistic approach to the problem.

---

2 See Mantelero, A. (2014) Social Control, Transparency and Participation in the Big Data World. Journal of Internet Law, forthcoming.

3 See Mayer-Schönberger, V. (1997). Generational development of data protection in Europe, in Agre, P., Rotenberg, M. (Eds.), Technology and privacy: The new landscape (pp. 219-241). Cambridge, Massachusetts: The MIT Press; Bygrave, Lee A. (2002). Data Protection Law. Approaching Its Rationale, Logic and Limits (pp. 93-169). The Hague, London, New York : Kluwer Law International.

4 In the U.S. the traditional approach, based on different sectorial regulations, underestimated the role played by user's choice, adopting a marked-oriented approach; nevertheless the recent guidelines adopted by the U.S. administrations seems to adopt a different approach, reinforcing self-determination, although these new set of principles are still unimplemented. See The White House. (2012). A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (pp. 47-48). Retrieved February, 28th, 2014 from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

5 See below para. 3.

6 See Cavoukian, A., Jonas, J. (2012). Privacy by Design in the Age of Big Data. Retrieved February, 28th, 2014 from http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf; Cavoukian, A., Reed, D. (2013). Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design. Retrieved February, 28th, 2014 from http://www.privacybydesign.ca/content/uploads/2013/12/pbd-big_privacy.pdf.

7 See Nissenbaum, H. (2010). Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

8 See Cate, F. H., Mayer-Schönberger, V. (2012). Notice and Consent in a World of Big Data. Microsoft Global Privacy Summit Summary Report and Outcomes. Retrieved February, 28th, 2014 from http://www.microsoft.com/en-au/download/details.aspx?id=35596.

In contrast, this article suggests the adoption of different solutions for situations in which the role of the consent-based model is outdated and the contexts in which the traditional model mainly based on opt-in can be preserved.

In doing so, the experience from the past should not be forgotten. In many cases, the first answer given by the legal system to new technological and social revolutions[9] is represented by the introduction of new ad hoc rules. Nevertheless, the lack of knowledge of past experiences makes it difficult to find adequate answers to the new questions that technology poses.

In the light of the above, this article reconsiders the history of data protection and its evolution from mainframe to Big Data, in order to give an answer to the contemporary problems of privacy and data protection. This is not a mere cultural interest in this historical perspective, since there are evidently a numbers of similarities between the context of the 50's-60's and the present. For this reason the analysis of that experience can offer elements to address the new challenges and to re-think the data protection framework.

2. THE REASONS OF DATA PROTECTION AND THE FIRST GENERATIONS OF REGULATIONS

Before considering the different reasons that induce the law to protect personal information, it should be noticed that European legal systems do not recognize the same broad notion of the right to privacy, which exists in U.S. case laws. At the same time, data protection laws in the European countries do not draw their origins from the European idea of privacy and its related case law.

With regard to the notion of right to privacy (and in brief), in the U.S. the right to privacy covers a broad area that goes from informational privacy to the right of self-determination in private life decisions. [10] On the other hand, in European countries this right mainly focuses on the first aspect and is related to the activities of the media.

With regard to the origins of data protection in Europe, it is worth pointing out that the European data protection regulations, since their origins in the late 60's, have

9 See Mayer-Schönberger, V., Cukier, K. (2013).

10 See Henkin, L. (1974). Privacy and Autonomy. Colum. L. Rev. 74, 1419; Wacks, R. (1980). The Poverty of «Privacy». Law Quarterly Review, 96, 77-78; Wacks, R.(1980). The Protection of Privacy (pp. 10-12). London: Sweet & Maxwell; Parent,W.A. (1983). A New Definition of Privacy for the Law. Law & Phil., 2, 305; Zimmerman, L.D. (1983). Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort. Cornell L.Rev., 68, 296, 299; Murphy, R.S. (1996). Property Rights in Personal Information: An Economic Defense of Privacy. Geo. L. J., 84, 2381.

focused on the information regarding individuals, without distinguishing between their public or private nature.[11] The right to privacy and data protection do not concern the same aspects, even if they are entangled and connected in many senses: there is only a partial overlapping, given that private facts are also referred to individuals, but at the same time a lot of personal information is publicly available and, for this reason, it does not fall into the field of the right to privacy. However, the legal issues related to the protection of personal information had a more recent recognition in law, both in the U.S. and Europe[12], dating from the 60's, whereas the primitive era of the right to privacy was at the end of 19th century when the penny press assumed a significant role in limiting the privacy of the people of upper classes[13]. For these reasons, our analysis should start from the computer revolution of the late 50's and not one century before, when the first decision on informational privacy were adopted in Europe[14], independently from the U.S. legal doctrine and before the milestone article of Warren and Brandeis.[15]

The first generations of data protection regulations were characterized by a national approach: regulations were adopted at different times and were different in the extension of the protection they provided and the remedies they offered.

The notion of data protection was originally based on the idea of control over information, as demonstrated by the literature of that period[16]. At that time, the migration from dusty paper archives to computer memories was a Copernican revolution which, for the first time in history, permitted the aggregation of information about every citizen previously spread over different archives. For this reason, the first regulations represented the answers given by legislators to the rising concern of citizens about social control as the introduction of big mainframe computers gave governments and big companies the opportunity to collect and manage large amount of personal information.[17]

---

11 See Costa, L., Poullet, Y. (2012). Privacy and the regulation of 2012. C. L. S. Rev. 28 (3), 255.

12 See fn. 3. See also Schwartz, P.M. (2013). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. Harv. L. Rev., 126, 1966, 1969-1992. Retrieved February, 28th, 2014 from http://www.harvardlawreview.org/media/pdf/vol126_schwartz.pdf.

13 See Schudson, M. (1978). Discovering the News: A Social History of American Newspapers. New York: Basic Books. See also below fn. 14 and 15.

14 See Trib. civ. Seine, 16 giugno 1858, D.P., 1858.3.62.

15 See Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. Harv. L. Rev., 4, 193.

16 See Westin, A. (1967). Privacy and Freedom. New York:Atheneum. See also Solove, J.D. (2008). Understanding Privacy (pp. 4-5). Cambridge, Massachusetts, London, England: Harvard Univerity Press.

17 See Bennett, C. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States (pp. 29-33). Ithaca, New York: Cornell University Press.

In that period, people were afraid of being visible like a gold fish in a glass bowl[18]. In the mainframe era a concentration of information, which was massive for the time, was in the hands of few entities, which were able to support the investments required by the new mainframe equipment. This concentration was also induced by the centralized architecture of mainframes, with their single central processing unit and a main memory in which all the computational power was placed and made available to other specialized terminals, which were connected.

The solution given by the legal systems was the opportunity to have a sort of counter-control over the collected data. The purpose of the regulations was not to spread and democratize power over information but to increase the level of transparency about data processing and guarantee the right to access to information. Citizens felt they were monitored and the law gave them the opportunity to know who controlled them, which kind of data were collected and for which purposes.

Technically speaking, a fundamental element of these new regulations were the mandatory notification to independent authorities of the creation of every new database and licensing, necessary in order to know who had control over information and to monitor data processing. Another key component of the first legal frameworks is the rights to access, which allowed citizens to ask the data owners about the way in which the information was used and, consequently, about their exercise of power over information. Finally, the entire picture was completed by the creation of ad hoc public authorities, to guarantee the respect and enforcement of citizen's rights, control over the data owners and the reaction against abuses.

In this model there was no space for individual consent, due to the economic context of that period. The collection of information was mainly made by public entities for purposes related to public interests, so it was mandatory and there was no space of autonomy in terms of negotiation about personal information. At the same time, personal information did not have an economic value for the private sector, as the data about clients and suppliers were only used for operational functions regarding the execution of the activities of the company.

Nevertheless, there was also another element that contributed to exclude the role of self-determination: the lack of knowledge, the extreme difficulty for ordinary people to understand how the mainframes worked. The computer mainframes were a sort of modern god, with sacral attendants, a selected number of technicians that was able to use this new equipment. In this scenario, it did not make sense to give citizens the chance to choose, since they were unable to understand the way in which the date was processed.

18 See Brenton, M. (1964). The Privacy Invaders. New York: Coward-McCann. See also Packard, V. (1964). The Naked Society. New York: David McKay; Miller, R.A. (1971). TheAssault on Privacy. Ann Arbor: The University of Michigan Press.

Finally, it is worth pointing out that all these aspects (concentration of information, centralised architecture, complexity of data processing) are now present again in the Big Data context, hence the practical relevance of this past experience, which will be more extensively considered in the following paragraphs.

3. THE NEW GENERATIONS OF REGULATIONS AND THE ECONOMIC VALUE OF PERSONAL INFORMATION

The following period –from the mid 70's to the 90's– can be considered as the era of distributed computers, in which a lot of people bought a personal computer to collect and process information. The big mainframe computers «became» the small desktop personal computer, with a relatively low cost. Consequently, the computational capacity was no longer an exclusive privilege of governments and big companies, but became accessible to many other entities and individual consumers.

This period witnessed another transformation involving direct marketing, which was no longer based on the concept of mail order and moved towards computerized direct marketing solutions.[19] The new forms of marketing were based on customer profiling and required extensive data collection to apply data mining software. The main purpose of profiling was to suggest a suitable commercial proposal to any single consumer. This was an innovative application of data processing driven by new purposes. Information was no longer collected to support supply chains, logistics and orders, but to sell the best product to single users. As a result, the data subject became the focus of the process and this information acquired an economic and business value, given its role in sales.

These changes in the technological and business frameworks created new requests from society to legislators since citizens wanted to have the chance to negotiate their personal data and gain something in return.

Although the new generations of the European data protection laws placed personal information in the context of fundamental rights[20], the main goal of these regulations

19 Although direct marketing has its roots in mail order services, which were based on personalized letter (e.g. using the name and surname of addressees) and general group profiling (e.g. using census information to group addressees in social and economic classes), the use of computer equipment increased the level of manipulation of consumer information and generated detailed consumer's profiles. See Petrison et al., 1997, 115-119 («During the decade, companies not only learned their customer's names and addresses, they also began to collect detailed personal and purchasing information, thereby beginning to understand them as individuals rather than as part of a traditional mass audience»).

20 See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981 and entered into force

was to pursue economic interests related to the free flow of personal data. This is also affirmed by the Directive 95/46/EC, which represents both the general framework and the synthesis of this second wave of data protection laws[21]. Nevertheless the roots of data protection still remained in the context of personality rights and, for this reason, the European approach is less market-oriented[22] than in other legal systems. The Directive also recognizes the fundamental role of public authorities in protecting data subjects against unwilled or unfair exploitation of their personal information for marketing purposes.

Both the theoretical model of fundamental rights, based on self-determination, and the rising data-driven economy highlighted the importance of user consent in data processing[23]. Consent does not only represent an expression of choice with regard to the use of personality rights by third parties, but is also an instrument to negotiate the economic value of personal information.[24] In this new data-driven economy, personal data cannot be exploited for business purposes without any involvement of the data subject. It is necessary that data subjects become part of the negotiation, since data are no longer

on 1st October 1985. Retrieved February, 28th, 2014 from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG; OECD, Annex to the Recommendation of the Council of 23rd September 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved February, 28th, 2014 from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface.

21 The EU Directive 95/46/EC has this bivalent nature, since it was written on the basis of the existing national data protection laws, in order to harmonize them, but at the same time it also provided a new set of rules. See the recitals in the preamble to the Directive 95/46/EC.

22 On the different approach based on the protection of personal data in terms of property, see Lessig, L. (1999). Code: And Other Laws of Cyberspace. New York: Basic Books; Samuelson, P. (2000). Privacy as Intellectual Property? Stan. L. Rev. 52, 1125; Schwartz, P.M. (2004). Property, Privacy and Personal Data Harv. L. Rev., 117, 2055. For criticism, see Cohen, J.E. (2000). Examined Lives: Informational Privacy and the Subject as an Object. Stan. L. Rev.. 52, 1373.

23 See Charter of Fundamental Rights of the European Union (2010/C 83/02), art. 8, OJEU, 30 March 2010, C83/389. See also Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, para. 63 s. Retrieved February, 28th, 2014 from http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-275/06&td=ALL; Bundesverfassungsgericht, 15 Decmber 1983, Neue Juristische Wochenschrift, 1984, 419 ss. Among the legal scholars, see also Schwartz, P.M. (2013). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. Harv. L. Rev. 126, 1966. Retrieved February, 28th, 2014 from http://www.harvardlawreview.org/media/pdf/vol126_schwartz.pdf; Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. International Data Privacy Law, 3 (2), 88.

24 See also Acquisti, A., Grossklags, J. (2005). Privacy and rationality in individual decision making. Security & Privacy, IEEE, 3(1), 26–33.

used mainly by government agencies for public purposes, but also by private companies with monetary revenues.[25]

Nevertheless, effective self-determination in data processing, both in terms of protection and economic exploitation of personality rights, cannot be obtained without adequate and prior notice. For these reasons, the «notice and consent» model[26] has added a new layer to the existing paradigm based on transparency and access.

Finally, it is important to highlight that during the 80's and 90's data analysis increased in quality but its level of complexity was still limited. Consequently users were still able to understand the general correlation between data collection and related purposes of data processing (e.g. profiling users, offering customized services or goods). Clearly, at that time, informed consent and self-determination were largely considered as synonyms. This changed in the future Big Data era.

4. THE FUTURE GENERATION OF REGULATIONS IN A CONTEXT CHARACTERIZED BY BIG DATA AND BIG PLAYERS

The present Big Data era is different from the previous period both in terms of economic and technological context, with direct consequences on the coherence of the legal framework adopted to protect personal information.

The new environment is mainly digital and characterized by an increasing concentration of information in the hands of a few entities, both publican and private. The role played by specific subjects in the generation of data flows is the principal reason for this concentration. Governments and big private companies collect huge amounts of data while performing their daily activities. This bulk of information represents a strategic and economically relevant asset, since the management of large databases enables these entities to assume the role of gatekeepers with regard to the information that can be extracted from the datasets, by limiting access to the data, perhaps to specific subjects only or to circumscribed parts of the entire collection, or by keeping it completely closed.

Not only governments and big private companies acquire this power, but also the intermediaries in information flows (e.g. search engines, Internet providers, credit re-

25 See OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing.

26 See Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation. Privacy & Sec. L. Rep., 11, 1, 5.
With regard to personal information collected by public entities, in various cases the Directive 95/45/EC allows data collection without the consent of data subject; however, the notice to data subjects is necessary also in these cases. See Articles 7, 8 and 10, Directive 95/46/EC.

port agencies, marketing companies), which do not generate information, but play a key role in circulating it.

There are also different cases in which information is accessible to the public, both in raw and processed form. This happens with regard to open data sets made available by government agencies, information held in public registries, data contained in reports, studies and other communications made by private companies and, finally, online user-generated contents, which represent a relevant and increasing portion of the information available online.

The concurrent effect of all these different sources only apparently diminishes the concentration of power over information, since access to information is not equivalent to knowledge. A large amount of data creates knowledge if the holders have the adequate interpretation tools to select relevant information, to reorganize it, to place the data in a systematic context and if there are people with the skills to define the design of the research and give an interpretation to the results generated by Big Data analytics.

Without these skills, data only produces confusion and less knowledge in the end, with information interpreted in an incomplete or biased way.

For these reasons, the availability of data is not sufficient in the Big Data context. It is also necessary to have the adequate human and computing resources to manage it. In this scenario, control over information does not only regard limited access data, but can also concern open data, over which the information intermediaries create an added value by means of their instruments of analysis.

Because only few entities are able to invest heavily in equipment and research, the dynamics described above enhance the concentration of power over information, which increases due to the new expansion of Big Data and its global dimension.

Under many aspects, this new environment resembles the origins of data processing, when in the mainframe era technologies were held by a few entities and data processing was too complex to be understood by data subjects. Could this suggest that, in the future, the scenario will change again in a sort of «distributed Big Data analytics», as it happened in the mid '70? Probably not. The new «data barons» do not base their position only on expensive hardware and software, which may become cheaper in the future. Neither is their position based on the growing number of staff with specific skills and knowledge, able to give an interpretation to the results of data analytics. The fundamental element of the power of «data barons» is represented by the large databases they have. These data silos, considered the goldmine of the 21st century, do not have free access, as they represent the main or the side-effect of the activities realized by their owners, due to the role they play in creating, collecting or managing information.

For this reason, with regard to Big Data, it does not seem so easy to imagine the same process of «democratization» that happened concerning computer equipment during the 80's: the access to the above mentioned large databases is not only protected by

legal rights, but it is also strictly related to the peculiar positions held by the data holders in their market and to the presence of entry barriers.

Another aspect that characterizes and distinguishes this new form of concentration of control over information is given by the nature of the purposes of data collection: data processing is no longer focused on single users (profiling), but it increased by scale and it trying to investigate attitudes and behaviours of large groups and communities, up to entire countries. The consequence of this large scale approach is the return of the fears about social surveillance, which characterized the mainframe era.

Nevertheless, it is important to highlight that this new potentially extensive and pervasive social surveillance differs from the past, since the modern surveillance is no longer realized only by intelligence apparatus, which autonomously collects a huge amount of information through pervasive monitoring systems. It is the result of the interplay between private and public sectors, based on a collaborative model made possible by mandatory disclosure orders, which are issued by courts or administrative bodies, and extended to an undefined pool of voluntary or proactive collaborations from big companies.[27] In this way, governments obtain information with the indirect «co-operation» of the users who probably would not have given the same information to public entities if requested. Service providers for example collect personal data on the base of private agreements (privacy policies) with the consent of the user and for specific purposes[28], but governments exploit this practice by using mandatory orders to obtain the disclosure of this information. This dual mechanism hides from citizens the risk and the dimension of the social control that can be realised by monitoring social networks or other services and using Big Data *analytics* technologies.[29]

---

27 See also Council of Europe (2008). Guidelines for the cooperation between law enforcement and internet service providers against cybercrime. Retrieved February, 28th, 2014 from http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf [Dec. 10, 2013].

28 On the linkage between data retention and access from government agencies or law enforcement authorities, see Reidenberg, J. (2013). The Data Surveillance State in the US and Europe. Wake Forest Law Review, forthcoming. Retrieved February, 28th, 2014 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269#!.

29 See European Parliament (2013). Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy. Retrieved February, 28th, 2014 from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (2013). The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens (pp. 14-16). Retrieved February, 28th, 2014 from http://info.publicintelligence.net/EU-NSA-Surveillance.pdf; European

In this scenario, the traditional data protection framework defined in the 90's goes to crisis[30], since the new technological and economic (i.e. market concentration, social and technological lock-ins) context undermined two of its fundamental pillars: the purpose specification and use limitation principles and the «notice and consent» model.

The purpose specification and use limitation principles have their roots in the first generations of data protection regulations, since they are strictly related to the intention of avoiding extensive data collections, which may imply risks in terms of social surveillance and control. With the advent of the new generation of data protection regulations –during the 80's and 90's–, these principles not only that represented a limit to data processing, but also became a key element of the «notice and choice» model, since they define the use of personal information made by data controllers that is an important information impacting users' choice. Nevertheless, the advent of Big Data analytics makes it difficult to provide detailed information about the purposes of data processing and the expected outputs. Since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more «evanescent», as a consequence of the «transformative»[31] use of Big Data, which makes it often impossible to explain all the possible uses of data at the time of its initial collection.

These critical aspects concerning the purpose specification limitation have a negative impact on the efficiency of the «notice and consent» model. First, the difficulty in defining the expected results of data processing induces introducing generic and vague statements in the notices about the purposes of data collection. Second, also in the

---

Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (2013). National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law (pp. 12-16). Retrieved February, 28th, 2014 from http://www.europarl.europa.eu/committees/it/libe/studiesdownload.html?languageDocument=EN&file=98290. See also DARPA (2002). Total Information Awareness Program (TIA). System Description Document (SDD), Version 1.1. Retrieved February, 28th, 2014 from http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf.

30 See Cate, F. H. (2006). The Failure of Fair Information Practice Principles. In Winn, J. (ed.), Consumer Protection in the Age of the Information Economy (pp. 343–345). Aldershot-Burlington: Ashgate. Retrieved February, 28th, 2014 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972. See also Cate, F.H., Mayer-Schönberger, V. (2012). Notice and Consent in a World of Big Data. Microsoft Global Privacy Summit Summary Report and Outcomes. Retrieved February, 28th, 2014 from http://www.microsoft.com/en-au/download/details.aspx?id=35596; Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 3 (2), 74-87.

31 See Tene, O., Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. Stan. L. Rev. Online 64, 64.

hypothesis of the adoption of long and detailed notices, the complexity of data processing in the Big Data environment does not offer to users a real chance to understand it and to make their choice.

Moreover, this scenario is made worse by the economic, social and technological constraints, which definitively undermine the idea of self-determination with regard to personal information that represented the core principle of the generation of data protection regulations approved during the 80's and 90's. As mentioned before, we assisted to an increasing concentration of the informational assets, due to the multinational or global nature of some big players of the new economy, but also due to merger and acquisition processes, which created big companies both in the online and offline markets. In various cases, mainly with regard to online services, these large scale trends drastically limit the number of the companies that provide specific kind of services, which consequently have hundreds of millions of users. This dimension of the dominant players also produces social and technological lock-in effects that increase data concentration and represents further direct and indirect limitations to user's self-determination and choice.[32]

In the described scenario, characterized by complex data processing and concentration of control over information, the decision to maintain a model mainly focused on «notice and choice» represents a risk, since it is easy for companies to give notice and require the consent without an effective self-determination of users, given the abovementioned reasons.

This leads us to reconsider the role of user's self-determination and to differentiate the situations in which users are not able to understand deeply the data processing and its purposes, or are not in the position to decide,[33] from the other different situations

32 A social lock-in effect exist in social networks as a consequence of the dominant position held by some big players, which intrinsically limits the user's possibility to recreate the same network elsewhere. For this reasons, this kind of lock-in also reduces user's propensity to change platform and limits their chances of not being profiled or tracked. The technological lock-in has a different nature: it is related to technological standards and data formats adopted by service providers and it limits the data portability and migration from one service to another, which offers the same functions.

33 See also Article 7 (4), Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012. Retrieved February, 28th, 2014 from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf («Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller»). In 2013, The Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament has dropped the former Article 7 (4), see Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (Gen-

in which they can take an actual, free and aware decision. With regards to the first hypothesis, there it seems to be an analogy between the characters of data processing in the Big Data era and what it happened in the mainframe age: like at the beginnings of computer age, today, data is collected by a limited number of entities and users are not able to understand the purposes and methods of data processing. In these cases the focus cannot be maintained mainly on the user and his or her self-determination: the role of users should be reduced and conversely the role of independent authorities should be increased. Data protection authorities, rather than users, have the technological knowledge to evaluate the risks associated to data processing and can adopt legal remedies to tackle them. Furthermore, they are also in the best position to balance all the different interests of the various stakeholders with regard to extensive projects of data collection and data mining.[34]

The suggestion is not to change the entire traditional model of data protection, but to reshape it with regard to the Big Data context and the other contexts in which asymmetries in data negotiation drastically reduce users' self-determination.[35] In the remaining cases, the «notice and consent» model, as traditionally designed, can still be effective, although it needs to be reinforced by increasing transparency, service provider's accountability and data protection-oriented architectures.[36]

5. A SUBSET OF RULES FOR BIG DATA AND LOCK-IN SITUATIONS

The context described above and the related observations suggest defining specific rules for Big Data uses and the situations characterized by asymmetries in data negotiation.[37] The necessity to distinguish this area seems not to be felt neither by the E.U.

---

eral Data Protection Regulation),(COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), compromise amendments on Articles 1-29 and on Articles 30-91 (hereinafter abbreviated as PGDPR-LIBE). Retrieved February, 28th, 2014 from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

34 See, e.g., Article 29 Working Party, Letter from the Article 29 Working Party addressed to Google regarding the upcoming change in their privacy policy, 2 February 2012. Retrieved February, 28th, 2014 from http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf.

35 See below para 5.

36 See Articles 13a, 23, 32a, 33, 33a, 34, 35, 39, PGDPR-LIBE.

37 For this reason, the following paragraphs will leave aside the cases in which users are able to understand the purposes of data collection and data processing, where the existing «notice and choice» and «purpose limited» consent can be kept valid.

legislator, in the proposal for a new data protection regulation, nor by the U.S. administration, in the Consumer Privacy Bill of Rights[38]. Although the E.U. proposal provides various rules that can be useful, it still adopts a holistic approach, in which the consent is still «purpose-limited»[39] and based on the «notice and choice» and the opt-in model.

Conversely, legal scholars and companies propose a different approach, which focuses on the use of the data, on the likely risks (of benefits and harms) associated with the proposed use of the data and on accountability.[40] This last approach has the undoubted merit to underline the crisis of the traditional model and to suggest a solution more suitable to address the issues of the existing and future context of data processing. Nevertheless it offers a holistic solution and this «one solution fits all» approach does not seem to be consistent with the different existing contexts, as above-mentioned.

With regard to Big Data, the new issues should not be necessarily addressed by making a choice between a «consent based» model and a «corporate accountability» model. Although Big Data and lock-in effects drastically limit self-determination at the moment in which the data are collected, the fundamental right of any person to decide about his or her own information cannot be erased and users should have the right to be informed about data processing and not to take part of it.

In this sense, the model here suggested is the result of the past experiences. Like in the first regulations of data protection regulations, the decision about data processing cannot be left to users, but at the same time user's rights to oppose to data processing and not to have personal data collected –codified in data protection laws during the 90's– should be preserved.

The fundamental pillars of this model are the adoption of the «opt-out» scheme and the definition of a rigorous data protection assessment, which should be publicly available. With regard to the latter, the same approach that is used in the field of product security and liability should be extended to data processing: in presence of complex data processing systems or data collections influenced by lock-in effects, the risk and benefit assessment should not be done by users, but it should be made by companies, under the supervision of data protection authorities. Users should only decide to exercise or not their right to opt-out.

---

38 See The White House (2012). A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (pp. 47-48). Retrieved February, 28th, 2014 from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

39 See Article 7 (4) Proposal.

40 See Cate, F.H., Mayer-Schönberger, V. (2013). Data Use and Impact. Global Workshop. Retrieved February, 28th, 2014 from http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf.

In this model, companies intend to adopt a strategy based on Big Data analytics should conduct a prior assessment of its impact on data protection, social surveillance and discrimination, in order to adopt all the adequate measures and standards to reduce it. This assessment, as in clinical trials, should be conducted by third parties and supervised by data protection authorities, which should also define the professional requirements of these third parties. Once the assessment is approved by data protection authorities, the process should be considered secure in terms of protection of personal information and risks of social surveillance or social discrimination and, for this reason, companies can enlist all users in the specific data processing, without any prior consent, but giving them a previous notice that mentions the results of the assessment[41] and providing them the opt-out option.

Obviously the entire system works only if the political and financial autonomy of data protection authorities, both from governments and corporations, is guaranteed. For this reason, it would be preferable a model based on mandatory fees paid by companies when they submit their requests of authorization to data protection authorities.

At the same time, in this model, independent authorities assume an important role in balancing all the different implications of data processing, not only in terms of data security but also in terms of social impact and ethical use of data. Conversely, a different assessment exclusively based on the adoption of security standards or corporate self-regulation would not have the same extent and independency. This does not mean that forms of standardization or co-regulation cannot be adopted;[42] nevertheless, the proposed reduction of the role of user's self-determination should have a necessary counterbalance in the active role of public and independent authorities acting in the interest of the whole society.

This model should offer clear and public procedures for assessment. These, undoubtedly, represent an economic burden for companies; nevertheless, in case of positive evaluation of data processing plans, these procedures allow companies to use data for complex and multiple purposes, without the inconvenience of acquiring a specific opt-in choice every time data is used for new purposes. Companies should only inform users about any changes and give them the chance to opt-out.

41 The notice should also describe how to access to the impact assessment report. This report is a short version of the documentation related to the assessment and it does not contain corporate sensitive information, in order to balance trade secrets and publicity of the assessment. Nevertheless, in presence of litigations, courts or data protection authorities may have access to the complete documentation and may disclose it to the compliant.

42 See Calo, R. (2013). Consumer Subject Review Boards: A Thought Experiment. Stan. L. Rev. Online 66, 97.

From the user's point of view, on the one hand, the assessment conducted by the data protection authorities on one hand gives them a guarantee of an effective evaluation of the risks related to data processing and, on the other hand, the opt-out allows them to receive information about data processing and to decide if they do not want to be part of the data collection.

6. BIBLIOGRAPHY

Acquisti, A., Grossklags, J. (2005). Privacy and rationality in individual decision making. Security & Privacy, IEEE, 3(1), 26–33.

Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (pp. 29-33). Ithaca,

Brenton, M. (1964). *The Privacy Invaders*. New York: Coward-McCann

Bygrave, Lee A. (2002). *Data Protection Law. Approaching Its Rationale, Logic and Limits* (pp. 93-169). The Hague, London, New York: Kluwer Law International.

Calo, R. (2013). Consumer Subject Review Boards: A Thought Experiment. *Stan. L. Rev. Online* 66, 97.

Cate, F. H. (2006). The Failure of Fair Information Practice Principles. In Winn, J. (ed.), *Consumer Protection in the Age of the Information Economy* (pp. 343–345). Aldershot-Burlington: Ashgate. Retrieved February, 28th, 2014 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

Cate, F.H., Mayer-Schönberger, V. (2012). *Notice and Consent in a World of Big Data. Microsoft Global Privacy Summit Summary Report and Outcomes*. Retrieved February, 28th, 2014 from http://www.microsoft.com/en-au/download/details.aspx?id=35596

Cate, F.H., Mayer-Schönberger, V. (2013). *Data Use and Impact. Global Workshop*. Retrieved February, 28th, 2014 from http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf.

Cavoukian, A., Jonas, J. (2012). *Privacy by Design in the Age of Big Data*. Retrieved February, 28th, 2014 from http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf

Cavoukian, A., Reed, D. (2013). *Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design*. Retrieved February, 28th, 2014 from http://www.privacybydesign.ca/content/uploads/2013/12/pbd-big_privacy.pdf

Cohen, J.E. (2000). Examined Lives: Informational Privacy and the Subject as an Object. *Stan. L. Rev.*. 52, 1373.

Costa, L., Poullet, Y. (2012). Privacy and the regulation of 2012. *C. L. S. Rev.* 28 (3), 254-262

Council of Europe (2008). *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*. Retrieved February, 28th, 2014 from http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981 and entered into force on 1st October 1985. Retrieved February, 28th, 2014 from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG

DARPA (2002). *Total Information Awareness Program (TIA). System Description Document (SDD), Version 1.1.* Retrieved February, 28th, 2014 from http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf.

European Parliament (2013). *Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*. Retrieved February, 28th, 2014 from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN

European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (2013). *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens* (pp. 14-16). Retrieved February, 28th, 2014 from http://info.publicintelligence.net/EU-NSA-Surveillance.pdf

European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (2013). National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law (pp. 12-16). Retrieved February, 28th, 2014 from http://www.europarl.europa.eu/committees/it/libe/studiesdownload.html?languageDocument=EN&file=98290.

Henkin, L. (1974). Privacy and Autonomy. Colum. L. Rev. 74, 1410-1433

Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation. *Privacy & Sec. L. Rep*., 11, 1, 5.

Lessig, L. (1999). *Code: And Other Laws of Cyberspace*. New York: Basic Books

Mantelero, A. (2014) Social Control, Transparency and Participation in the Big Data World. *Journal of Internet Law*, forthcoming.

Mayer-Schönberger, V. (1997). Generational development of data protection in Europe, in Agre, P., Rotenberg, M. (Eds.), *Technology and privacy: The new landscape* (pp. 219-241). Cambridge, Massachusetts: The MIT Press

Mayer-Schönberger, V., Cukier, K. (2013). *Big Data. A revolution That Will Transform How We Live, Work and Think* (p. 182). London: Jhon Murray.

Miller, R.A. (1971). *TheAssault on Privacy*. Ann Arbor: The University of Michigan Press.

Murphy, R.S. (1996). Property Rights in Personal Information: An Economic Defense of Privacy. Geo. L. J., 84, 2381. New York: Cornell University Press.

Nissenbaum, H. (2010). *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press

OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, OECD Publishing.

OECD, Annex to the Recommendation of the Council of 23rd September 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved February, 28th, 2014 from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface.

Packard, V. (1964). *The Naked Society*. New York: David McKay

Parent,W.A. (1983). A New Definition of Privacy for the Law. *Law & Phil*., 2, 305-338

Reidenberg, J. (2013). The Data Surveillance State in the US and Europe. *Wake Forest Law Review*, forthcoming. Retrieved February, 28th, 2014 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269#!.

Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, 3 (2), 74-87.

Samuelson, P. (2000). Privacy as Intellectual Property? *Stan. L. Rev*. 52, 1125

Schudson, M. (1978). *Discovering the News: A Social History of American Newspapers*. New York: Basic Books

Schwartz, P.M. (2004). Property, Privacy and Personal Data *Harv. L. Rev*., 117, 2055

Schwartz, P.M. (2013). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. *Harv. L. Rev*. 126, 1966. Retrieved February, 28th, 2014 from http://www.harvardlawreview.org/media/pdf/vol126_schwartz.pdf

Schwartz, P.M. (2013). The E.U.-US Privacy Collision: A Turn to Institutions and Procedures. *Harv. L. Rev*., 126, 1966, 1969-1992. Retrieved February, 28th, 2014 from http://www.harvardlawreview.org/media/pdf/vol126_schwartz.pdf.

Solove, J.D. (2008). *Understanding Privacy*. Cambridge, Massachusetts, London, England: Harvard University Press.

Tene, O., Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stan. L. Rev. Online* 64, 64.

The White House (2012). *A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Retrieved February, 28th, 2014 from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, 3 (2), 88.

Wacks, R. (1980). The Poverty of «Privacy». Law Quarterly Review, 96, pp. 73-78

Wacks, R.(1980). *The Protection of Privacy* (pp. 10-12). London: Sweet & Maxwell

Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harv. L. Rev.*, 4, 193.

Westin, A. (1967). *Privacy and Freedom*. New York:Atheneum

Zimmerman, L.D. (1983). Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort. *Cornell L.Rev.*, 68, 296-365

12

HOW UNINFORMED IS THE AVERAGE DATA SUBJECT? A QUEST FOR BENCHMARKS IN EU PERSONAL DATA PROTECTION

Gloria González Fuster
Law, Science, Technology and Society (LSTS)
Vrije Universiteit Brussel (VUB)
Researcher

ABSTRACT: Information obligations have always been crucial in personal data protection law. Reinforcing these obligations is one of the priorities of the legislative package introduced in 2012 by the European Commission to redefine the personal data protection legal landscape of the European Union (EU). Those responsible for processing personal data (the data controllers) must imperatively convey certain pieces of information to those whose data are processed (the data subjects), and they are expected to do so in an increasingly 'transparent' manner. Beyond these punctual information requirements, however, data subjects appear to always be and inevitably remain in a state of relative ignorance, as in almost constant need of further guidance. Data subjects are nowadays often depicted as unknowing consumers of online services, services which surreptitiously take away from them personal data thus conceived as a valuable asset. In light of these developments, this contribution critically investigates how is EU law envisaging data subjects in terms of knowledge. The paper reviews the birth and evolution of information obligations as an element of European personal data protection law, and asks whether thinking of data subjects as consumers is consistent with the notion of 'average consumer' functioning in EU consumer law. Finally, it argues that time might have come to openly clarify when are data subjects unlawfully misinformed, and that, in the meantime, individuals might benefit not only from accessing more 'transparent' information, but also from being made more aware of the limitations of the information available to them.

KEYWORDS: Data protection, transparency, European Union, data subject, privacy, information, average consumer.

1. INTRODUCTION

Individuals are not properly informed about the processing of personal data about them. This recurrent statement can hide behind its apparent simplicity many different assumptions. It can be used to justify the need for (better) laws on privacy and personal data protection, or, on the contrary, to prove their limitations or ineffectiveness. It can be presented as a problem to be tackled imposing obligations on those who process data (the data processors) to inform those whose data are processed (the data subjects), but it can also be viewed as a proof of a persistent resistance of such data processors to provide data subjects with the full picture of what is happening to the data about them.

This contribution[1] investigates how are envisaged data subjects in relation to knowledge in European Union (EU) law. It looks for references useful to assess to which extent individuals are supposed to be informed or uninformed about data processing practices concerning them, as well as to understand the conceptualisations and operationalizations of such (mis)information. To this purpose, the paper first offers a brief historical review situating the roots of the recognition of individual's lack of knowledge at the very origins of personal data protection. This is followed by a review of information obligations of data processors and their relation with fairness and transparency. Is then introduced the increasingly popular conception of data subjects as consumers, which leads to an inquiry into the possible applicability of the legal notion of 'average consumer' in the context of EU data protection law.

2. (FOREVER) INFORMING THE DATA SUBJECT

The idea that individuals must be informed when data about them are processed saw the light already in the 1960s. Historically, the surfacing of modern notions of privacy and personal data protection was precisely based on a perception of a dangerous loss of control and lack of awareness suffered by citizens due to the advent of computerisation. This feeling of disorientation and disempowering[2] was eventually described as resulting from a 'knowledge asymmetry' between those managing vast quantities of data and those whose data are processed.[3] Privacy and personal data protection were thus promoted as legal tools enabling individuals to counter loss of control upon what happens to data concerning them.

2.1. Early recognition

When Alan F. Westin put forward his powerful vision of privacy as control upon personal information,[4] he was indeed reacting to the realisation that computers, and especially large databases, threatened to deprive individuals of any effective oversight of the fate of data about them when in the hands of others. In 1973, an influential report

---

1 The present research has been carried out in the context of the EU-funded project *Privacy and Security Mirrors* (PRISMS).

2 Bygrave, L. A. (2002). *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague: Kluwer Law International, p. 107.

3 See, notably: Hildebrandt, M. and Koops, B. J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *The Modern Law Review, 73 (3*), 428-460.

4 Westin, A. F. (1970, originally published in 1967). *Privacy and Freedom.* New York: Atheneum.

warned of the lessening of individuals' control upon data in the United States (US), and proposed a set of recommendations to mitigate this problem. One of them was the general prohibition of secret record keeping systems.[5]

In France, since 1978 individuals have the right to be informed about any data used in automated processing practices affecting them. Since then, citizens are also entitled to receive information whenever somebody asks them for data, such as who are the recipients.[6] In Germany, in 1983 the German Federal Constitutional Court recognised a fundamental right to informational self-determination, and did so by emphatically noting that such right is incompatible with a society where citizens do not know who knows what about them.[7]

International data protection instruments have always imposed information obligations on those who process data. In 1980, the Organisation for Economic Co-operation and Development (OECD) set out in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data the 'openness principle'. According to this principle, there must be 'a general policy of openness about developments, practices and policies with respect to personal data', whereby, whenever personal data are processed, individuals should be able to establish the existence and nature of such data, the main purposes of their use, who are the data controllers, and where to find them.[8] In the OECD Guidelines, the 'openness principle' functions as a prerequisite for the 'individual participation principle', which grants individuals a right to access information about data concerning them held by others.[9] In addition, the 'collection limitation principle' states that, as a general rule, collection of data must occur with the knowledge of the data subject.[10]

In 1981, Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[11] prescribed that

5 Secretary's Advisory Committee on Automated Personal Data Systems (1973). *Records, Computers and the Rights of Citizens*.

6 *Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier* 1978, see Arts. 3 and 27.

7 *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff. Describing this right as a right to control the use of information about oneself: Whitman, J Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal, 113,* 1151–1221, p. 1161.

8 Annex to the Recommendation of the Council of 23 September 1980: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, § 12.

9 OECD Guidelines, § 13 and § 27.

10 Ibid., § 7.

11 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg, 28.I.1981.

everybody shall 'be enabled to establish the existence' of any automated data files containing data about them, as well as the 'main purposes' of such files, and the residence, or place of business, of the file's controller.[12] Furthermore, individuals were entitled to obtain confirmation of whether data about them are stored by controllers, and a right to communication of the data.[13]

All in all, these developments describe the progressive incorporation into privacy and personal data protection laws of a certain right to know, as one of the components of a set of measures aimed at compensating a risk of loss of control upon data suffered by individuals. This right to know emerges thus as a key to reduce 'deficits in data subjects' cognitive sovereignty'.[14] This right does not correlate exactly with the duty to inform of data controllers,[15] as it can also be addressed through other means.[16] Importantly, however, the perceived lack of knowledge is not remedied by privacy and personal data protection laws, as various interlinked 'cognitive problems'[17] appear to persist and always seem to bring back to the reality of the 'uninformed individual'.[18]

2.2. Existing obligations

The right to personal data protection has nowadays the status of fundamental right of the EU. It is recognised as such by Article 8 of the EU Charter of Fundamental Rights, a provision that, however, does not refer explicitly to any right to know, or even to any duty to inform.[19] Despite this formal absence, a right to receive information can be regarded as implicitly acknowledged by the statement of the Charter's Article 8 according to which personal data must be processed fairly, when read in conjunction

12 Art. 8(a) of Convention 108.

13 Ibid., Art. 8(b).

14 Bygrave, op. cit., p. 111.

15 In relation to the Spanish fundamental right to personal data protection, the Spanish Constitutional Court has alluded to the existence of both a right to know and a right to be informed of the use of data and its purpose (see § 6 of Sentencia 292/2000, de 30 de noviembre de 2000).

16 For example, early national laws gave great importance to the notification of data processing practices to supervisory authorities, and to the availability of public registers, which aim generally to increase public awareness of those practices.

17 Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. 126 *Harvard Law Review* 1880; GWU Legal Studies Research Paper No. 2012-141 p. 1888.

18 Ibid., p. 1883.

19 Ruiz, M. C. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo, 7(14),* 7–43, p. 39.

with EU's main instrument on personal data protection, Directive 95/46/EC (the 'Data Protection Directive').[20]

The Data Protection Directive indeed sets out that personal data must be processed fairly and lawfully,[21] and its preamble observes that, for the processing to be fair, 'the data subject must be in a position to learn of the existence of a processing operation'.[22] The preamble goes on to clarify that data subjects must be given accurate and full information when data are collected, or when used in a way that could not have been anticipated at the time of collection.[23] Hence, Directive 95/46/EC connects the data controller's duty to inform to the requirement of fair processing.

The Directive's provisions establishing obligations to inform, namely Articles 10 and 11, corroborate this link. They mark a distinction between compulsory information (such as the controller's identity, and the purposes of the data processing) and some 'further information' only required in some cases. Such 'further information' concerns the identification of the recipients of the data, and the existence of a right of access and a right to rectify, and must be given only when, having regard to the specific circumstances of the processing, it is required to guarantee fair processing.

These provisions on information obligations have been commonly labelled 'transparency' measures,[24] even if Directive 95/46/EC does not use the term transparency in this context.[25] Accepting the labelling, transparency can be described 'a pre-condition to fair processing',[26] and the data controllers' duty to inform[27] may be depicted as a 'crucial

20 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31-50.

21 Art. 6(a) of Directive 95/46/EC.

22 Recital 38 of Directive 95/46/EC.

23 Recitals 38, 39 and 40 of Directive 95/46/EC.

24 ICO (2009). *The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data*. On transparency as an element of fairness, see: Kuczerawy, A. and Coudert, F. (2011). Privacy Settings in Social Networking Sites: Is It Fair. In Simone Fisher-Hübner et al. (eds.), *Privacy and Identity Management for Life*, International Federation for Information Processing (IFIP), 237-238, and Bygrave, op. cit., pp. 58-59.

25 Actually Directive 95/46/EC never uses the term transparency, except once in the preamble, concerning the obligation of national supervisory authorities to publish annual reports (Recital 63).

26 Art. 29 Working Party (2009). *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. WP 168, p. 8.

27 EU Agency for Fundamental Rights and Council of Europe (2014). *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the EU, p. 99.

measure' to promote transparency.[28] Insofar as it as an element of fair processing, in any case, the data controller's duty to inform may also be accepted as an integral part of the EU fundamental right to personal data protection.

A certain right to information can moreover be regarded as derived from the recognition in Article 8 of the EU Charter of a right to access and rectify data, both presented as constitutive elements of the EU fundamental right to personal data protection. To exercise such rights, data subjects need to be aware, first, of the fact that somebody is or might be processing data about them, and, second, of the fact that they enjoy the rights in question. Awareness of both issues is thus to some extent instrumental to the exercise of their rights.

Finally, Article 8 of the EU Charter refers also to the possibility to ground the legitimacy of data processing on the consent of the data subject. This brings in another link between the right to personal data protection and information requirements, as, to be valid, consent must be 'informed'. The Data Protection Directive defines indeed consent as a 'freely given specific and informed indication' of the data subject's wishes signifying agreement to the processing of personal data.[29]

2.3. A need to inform more and better

Already more than a decade ago, the European Commission's first report on the implementation of the Data Protection Directive[30] concluded that the Directive's provisions on the data controllers' duty to inform were being put into effect across the EU in very divergent ways, and sometimes incorrectly. In 2004, European data protection authorities put under the spotlight the proliferation of inappropriate online notices, accused of being often 'very long' and containing 'legal terms and industry jargon'.[31] They called for more 'readable' formats,[32] and expressed support for multi-layered notices, which comprise a condensed notice from which can be reached more detailed information.[33]

2.3.1. Towards a new transparency

In 2009 the European Commission formally inaugurated the review of Directive 95/46/EC. A 2009 study sponsored by the United Kingdom's Information

28 Analysis and impact study on the implementation of Directive EC 95/46 in Member States accompanying European Commission's *First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003, COM (2003) 265 final, p. 19.

29 Art. 2(h) of Directive 95/46/EC.

30 COM (2003) 265 final.

31 Art. 29 Working Party (2004). *Opinion 10/2004 on More Harmonised Information Provisions*. WP 100, p. 5.

32 WP 100, p. 5.

33 Ibid., p. 4 and 6.

Commissioner's Office (ICO) corroborated that there was a problem with the Directive's information obligations, and argued that one of the main aspects of the problem was the way in which 'privacy policies' were being written.[34] The report stressed that, according to statistics, consumers felt strongly that mechanisms in place did not help them to understand their rights.[35]

In 2010, the European Commission published a Communication delineating its approach to the future of EU personal data protection.[36] Here, transparency was presented as 'a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data'.[37] The Communication advanced as a basic element of such transparency that information to data subjects must be 'easily accessible and easy to understand, and that clear and plain language is used'.[38] It observed that this was particularly relevant in the online environment, where privacy notices are often unclear and 'non-transparent', as allegedly proved by the results of a survey.[39] To tackle this problem, the European Commission announced that it would consider introducing in EU law 'a general principle of transparent processing of personal data'.[40]

The 2010 Communication thus set in motion a subtle change in the meaning of 'transparency' as a principle of EU data protection law. Whereas transparency had been traditionally understood as a principle implied in the principle of fair processing, encompassing a series of substantive requirements applicable to the data controller's duty to inform, it started then to acquire an additional sense, primarily concerned with the form in which information is to be delivered to data subjects. A sort of new transparency was seeing the light.

Still in the name of transparency, children were portrayed as deserving special consideration, because 'they may be less aware of risks, consequences, safeguards and rights

34 Robinson, N. et al. (2009), *Review of the European Data Protection Directive*, RAND Europe, p. 26.

35 Ibid., p. 29. In another section the same study states that the interest and awareness of consumers have been demonstrated, citing another survey (p. 25).

36 European Commission (2010), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union.* Brussels, 4.11.2010, COM(2010) 609 final.

37 COM(2010) 609 final, p. 6.

38 Idem.

39 Idem.

40 Idem. During the elaboration of its proposal, the European Commission received input from 'many respondents' alerting of the fact that transparency was already an integral part of EU data protection (see *Annex 4 accompanying the Impact Assessment: Summary of Replies to the Public Consultation on the Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union*, p. 56).

in relation to the processing of personal data',[41] thus requiring specific information practices. On top of that, the European Commission warned that it might contemplate drawing up EU standard forms, or harmonised 'privacy information notices'.[42]

In parallel to these measures targeting transparency, the 2010 Communication articulated a need to raise awareness, particularly among young people.[43] The boundaries between transparency and awareness-raising were rather vague: for instance, 'the provision of clear information on web-sites' was depicted as pursuing both.[44] As a matter of fact, the European Commission appeared concerned with the proliferation of opaque privacy notices in general, raising also the question of its impact on the very possibility for individuals to give informed consent to data processing practices.[45]

2.3.2. Proposal on the table: The new transparency principle

The European Commission presented in 2012 its proposal for a General Data Protection Regulation, designed to replace Directive 95/46/EC.[46] According to the Explanatory Memorandum accompanying the text, it introduces a new 'transparency principle',[47] which is not defined. The principle primarily takes the shape of a general declaration that personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'[48].

The proposal has a Chapter on the Rights of the Data Subject, with a Section titled 'Transparency and modalities'. This Section opens with Article 11, on 'Transparent information and communication', foreseeing that controllers 'shall have transparent and easily accessible policies[49] with regard to the processing of personal data and for the

41 COM(2010) 609 final, p. 6.

42 Idem.

43 Ibid., p. 8.

44 Idem.

45 Idem.

46 European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*). Brussels, 25.1.2012, COM(2012) 11 final.

47 Ibid., p. 8, where it is presented as a 'new element'.

48 Art. 5(a) of the proposed Regulation (cf. Art. 6(1)(a) of Directive 95/46/EC, stating that personal data must be 'processed fairly and lawfully').

49 'Privacy policies' appears to be used here in the sense of 'privacy notice', or texts destined to the users of services (on the meanings of the term: Van Alsenoy, B. (2012). *D6.1: Legal Requirements for Privacy-Friendly Model Privacy Policies*. Security and Privacy in Online Social Networks (SPION), p. 4).

exercise of data subjects' rights',[50] and that any information to data subjects shall be provided 'in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child'.[51] According to the proposed General Data Protection Regulation, therefore, the notion of transparent information should translate into easily accessible and (in spite of the tautology) transparent policies.

The substance of data controller's duty to inform is drawn up in the Section 'Information and access to data', that the proposal's preamble connects to the principles of fair and transparent processing.[52] This section specifies the information to be given to data subjects,[53] extending minimum requirements to include informing about the period of storage of data, and making it compulsory to notify the existence of a right to access and to rectify,[54] as well as of a right to lodge a complaint to a supervisory authority.[55] This is to be complemented with 'any further information necessary to guarantee fair processing in respect of the data subject'.[56]

The European Commission also advances that it may adopt implementing acts laying down standard forms for providing information to data subjects, 'taking into account the specific characteristics and needs of various sectors and data processing situations where necessary'.[57] The suggestion, however, has been publicly opposed by the Article 29 Working Party, which considers it unnecessary,[58] and also failed to find the support of the European Parliament.[59]

---

50 Art. 11(1) of the Proposed Regulation.

51 Ibid., Art. 11(2). This provision is inspired by the 2009 Madrid Resolution on International Standards on the Protection of Personal Data and Privacy, where the 'openness principle' was developed indicating that information to the data subject must be provided 'in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors', and by a provision proposed for a future Regulation on a Common European Sales Law, concerned with the duty to provide information when concluding distance contracts.

52 Recital (48) of the proposed Regulation.

53 For applicable exemptions, see Art. 14(5) of the Proposed Regulation.

54 Ibid., Art. 14(1)(d).

55 Ibid., Art. 14(1)(e).

56 Ibid., Art. 14(1)(h).

57 Ibid., Art. 14(8).

58 Art. 29 Working Party (2013). *Working Document 01/2013: Input on the proposed implementing acts*, WP 200, p. 6.

59 Amendment 110 of European Parliament's Resolution of 12 March 2014, P7_TA-PROV(2014)2012.

According to the impact assessment prepared by the European Commission before proposing its draft for the General Data Protection Regulation,[60] data subjects are generally unaware of the risks linked to personal data processing, and they thus fail to take appropriate measures to protect their personal data.[61] Of all data subjects, children are the most unaware of the risks at stake, which are however considerable, especially for them: '(i)n particular for young people', the impact assessment states, 'the disclosure of personal data can cause immense social and mental harm'.[62] It is not clear, however, how any increased awareness of children of the risks at stake might be capable of affecting their protection, as according to the proposed Regulation children are not to decide whether they consent or not to data processing practices. The decision is entrusted to the authorised parent or custodian.[63]

Globally speaking, the discussions on the draft General Data Protection Regulation hint towards a reinforcement of information obligations, regarding both the content of the information and formal requirements (in the spirit of the 'new' transparency). They also suggest a strengthening of the conceptual link between being informed and exercising data subject's rights. In parallel to all this emphasis on the need of individuals to be better informed, EU institutions are increasingly promoting the idea that data subjects, when disclosing personal data, shall be protected as consumers presumably trapped in a situation that very much escapes them.

3. A PORTRAIT OF THE DATA SUBJECT AS A CONSUMER

There is no doubt that consumers, and most notably online consumers, might also be regarded as data subjects insofar as, when consuming, they engage in communicating or making available data about them. In addition to this, however, data subjects are more and more often portrayed as being consumers whenever data about them is collected in exchange of access to free online services. This image is used to stress that

60 European Commission, Staff Working Paper: Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, SEC(2012) 72 final, p. 22.

61 SEC(2012) 72 final, p. 23.

62 Ibid., p. 29.

63 Art. 8 of the proposed Regulation.

free online services might not be as free as they look, because the data that is collected through them about individuals has a certain economic value.

The rationale behind the image of the data subject as a consumer is thus intrinsically tied to a depiction of users as typically uninformed and confused about the nature of the services they use, and hence misinterpreting their own behaviour. According to the impact assessment for the proposed General Data Protection Regulation, some individuals simply do not realise that many free online services rely on the processing of their personal data.[64] In this sense, some data subjects appear to be ill informed up to the point of misconceiving the very way in which online services function, leading them to engage in inattentive and incautious data practices.

Individuals would indeed not only be unaware of the fact that when using certain services they are celebrating in a way an economical transaction, but also ignorant of the price they are paying for it. An increasingly pervasive mantra depicts personal data as the new currency of the digital age,[65] and, concomitantly, consenting to the collection of personal data is conceived of as an exchange, where access to services is traded with data that hence constitutes an asset. This mantra is sustained by research studying how individuals decide to disclose or not personal data from the perspective of behavioural economics.[66]

The depiction of data subjects as consumers is sometimes put forward to promote the need to reinforce the protection of users of online services, notably by resorting to safeguards and notions borrowed from consumer law.[67] Taking this step, nevertheless, requires a prior careful examination of how are consumers actually envisaged in consumer law.

3.1. The average consumer

EU law protects consumers through different instruments, and, in some areas, it is guided by the ideal of the 'average consumer'. This notion originally emerged in the

64 SEC(2012) 72 final, p. 22.

65 Noting this trend in EU policy: Wauters, E., Lievens, E. and Valcke, P. (2013). *D1.2.4: A Legal Analysis of Terms of Use of Social Networking Sites, Including a Practical Legal Guide for Users: Rights & Obligations in a Social Media Environment.* User Empowerment in a Social Media Culture (EMSOC).

66 See, for instance: Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce, New York, May 17 - 20, 2004*, 21-29, doi>10.1145/988772.988777; Brandimarte, L., Acquisti A. and Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4: 340, DOI: 10.1177/1948550612455931.

67 See: European Data Protection Supervisor (EDPS) (2014). *Preliminary Opinion of the EDPS: Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, March.

case law of the EU Court of Justice[68] in connection with the free movement of goods, labelling and misleading advertising; further delineated in cases about trademark infringement, it eventually integrated EU secondary law.[69] Currently, the notion is notably employed in EU law to define 'misleading' commercial practices, which shall be regarded as misleading if they would mislead an average consumer.[70]

3.1.1. Reasonably well informed, observant and circumspect

The average consumer is a theoretical figure described as reasonably well informed and reasonably observant and circumspect, even if this depiction can vary taking into account social, cultural and linguistic factors.[71] The average consumer is regarded as a critical consumer, as opposed to a naïf consumer who would believe, for instance, any promotional marking tricks.[72]

Reliance on the figure the average consumer is supposed to help striking a fair balance between the need to protect consumers and promoting free trade. By discarding the idea that consumers are, as a general rule, weak, credulous or in need of help, it is possible to refute the validity of a number of protective measures that could be perceived as unjustified trade barriers.[73] From this viewpoint, the birth of the average consumer has been described as a move away from a paternalistic view of consumer law.[74]

The average consumer test is never a statistical test. Courts and responsible authorities must always exercise their own faculty of judgement, having regard to the case law of the EU Court of Justice, to determine the typical reaction of the average consumer in a given case.[75] In principle, they should not need to commission any expert's report

68 See: Case C-210/96, *Gut Springenheide and Tusky* (1998) ECR I-4657, para 31.

69 Incardona R. and Poncibò, C. (2007). The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution. *J Consum Policy 30*, 21–38, p. 22. See also: Regulation (EC) No 1924/2006 of the European Parliament and the Council of 20 December 2006 on nutrition and health claims made on foods, OJ L 404, 30.12.2006.

70 Van der Meulen, B. and Van der Velde, M. (2011). *European Food Law Handbook*. The Netherlands: Wageningen Academic Publishers, p. 421.

71 European Commission (2009). *Commission Staff Working Document: Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*, Brussels, SEC(2009) 1666, pp. 25-28.

72 Case C-470/93, *Verien gegen Unwesen in Handel und Gewerbe Koln e. V. v Mars GmbH* (1995) ECR I-01923, para 24.

73 SEC(2009) 1666, p. 25.

74 Incardona and Poncibò, op. cit., p. 22.

75 SEC(2009) 1666, p. 25.

or consumer research poll.[76] It will ultimately always be up to courts and responsible authorities to determine the percentage of consumers misled by a measure sufficiently significant to justify prohibiting such measure,[77] remembering that surveys results are subject to the frailties inherent in the formulation of survey questionnaires.[78] The notion of the average consumer as a reasonably well informed individual has been widely used in the area of food law regardless of the fact that many studies have demonstrated that an important number of consumers are unable to actually understand much of the information on food labels.[79]

3.1.2. Actively looking for information to make the right choices

The prototypical average consumer has an attitude that contributes to the constant improvement of knowledge:[80] always ready to obtain more information to make efficient choices, always in a position to acquire available information, and to act wisely on it.[81] On the basis of this conception of the average consumer, the EU Court of Justice considers that it is generally preferable to provide information to consumers so they can make their own choices, instead of trying to think on their behalf.[82] Information appears thus in the context of EU consumer law as a tool placed in the hands of consumers to enable them to decide freely.[83]

3.1.3. Not an obstacle to protect vulnerable consumers

Taking generally as a benchmark the average consumer is not incompatible with the protection of especially vulnerable consumers. Vulnerable consumers are recognised as existing, even if they are not regarded as the norm. Where a practice specifically tar-

76 Ibid., p. 28.

77 Case C-220/98, *Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH* (2000) ECR I-00117, para 31.

78 Opinion of Advocate General Fenelly for Case C-220/98, para 29.

79 MacMaoláin, C. (2007). *EU Food Law: Protecting Consumers and Health in a Common Market*, Oxford: Hart Publishing, p. 78.

80 Identifying attitude and knowledge as basic elements of the average consumer: González Vaqué, L. (2005). La noción de consumidor en el Derecho comunitario del consume. *Estudios sobre consumo*, *75,* 25-42.

81 SEC(2009) 1666, p. 25.

82 Van der Meulen and Van der Velde, op. cit., p. 422.

83 See, for instance, Art. 3(1) of Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, OJ L 304, 22.11.2011, 18-63.

gets a particular group of consumers, it is desirable that the impact of the practice be assessed from the perspective of the average member of that specific group.[84] According to EU consumer law, individuals can be particularly vulnerable because of a mental or physical infirmity, because of their age (notably, the elderly, children and teenagers), or because of their credulity. [85]

The vulnerable consumer test applies when it is foreseeable that a practice will affect the economic behaviour of a group of consumers. Hence, companies are only responsible for the negative impact of their practices on vulnerable consumers if they could reasonable expect such impact, and if they fail to take steps to mitigate it.[86]

3.2. Re-constructing the standard data subject

The described sketch of the average consumer makes visible some important frictions between this notion and the way in which the concept of data subject operates in EU law. First and foremost, it seems extremely difficult to maintain that the data subject is regarded in EU law, by default, as being well informed. On the contrary, as noted above, one the elementary assumptions behind the emergence of personal data protection law is that individuals lack enough knowledge on data processing practices affecting them, or are on the verge of losing control upon data. Data subjects appear to be originally and generally deprived of a satisfactory level of information. Once some pieces of information have been transmitted to them, the processing of their personal data might be regarded as fair, and they shall be able to make punctual informed decisions on whether to consent to some practices, but generally speaking they remain predominantly uninformed.

Information provided to individuals shall allow them to decide whether to consent or not,[87] but it is not envisaged as generally contributing to making choices between data processing options. In *Deutsche Telekom*,[88] the EU Court of Justice had to clarify whether, when an undertaking responsible for assigning telephone numbers wishes to pass on personal data on subscribers to a company providing publicly available directories, it is necessary for the undertaking to rely on the subscriber's consent, or on the

84 SEC(2009) 1666, p. 28.

85 Ibid., p. 29.

86 Ibid., p. 31.

87 Expressing awareness of some data processing practices does not equal consenting to them. See, notably: Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 9 November 2010, paras 61-64 and 88, as well as the Opinion of Advocate General Sharpston delivered on 17 June 2010, Joined Cases C-92/09 and C-93/09, para 77.

88 Case C-543/09 *Deutsche Telekom*, 5 May 2011.

subscriber's lack of objection.[89] The Court of Justice, analysing Directive 2002/58/EC,[90] stated that its provisions do not establish a 'selective right' of subscribers to decide in favour of certain providers of public directories. And the Court went on to add that when subscribers consent to their data being published in a directory with a specific purpose, assuming the 'detrimental' impact of such decision,[91] they will 'generally not have standing to object to the publication of the same data in another, similar directory'.[92]

Individuals' level of knowledge is very closely linked to their attitude towards information. Data subjects do not appear to be especially zealous to acquire more information, particularly when they are online, and might thus probably not be described as observant and circumspect. The appreciation of the eagerness of the data subject towards seeking information can affect the way in which information obligations are designed. In this context, multi-layered notices open the question of the extent to which information that is not given in a first layer, but only indirectly received or made available, has been received or made available at all. In 2012, the EU Court of Justice ruled that, in the context of distance contracts, consumer protection obligations compel to assess that where information that should be provided on a seller's website is made accessible only via a link sent to consumers, that information is neither 'given' to consumers, nor 'received' by them, for the purposes of EU law.[93]

3.3. A confused consumer and disoriented policy-making?

Against this background, it appears that configuring the data subject as a consumer has some important conceptual drawbacks. In the name of the alleged persistent misconceptions affecting the behaviour of online users, who seemingly indulge in using 'free' online services that in reality might not be free, data subjects are pushed towards a field of law where individuals are actually portrayed as by default well informed, observant and circumspect, and thus offered somehow limited protection. This brings to a paradoxical situation in which, because they are regarded as ignorant of how the Internet functions, individuals might qualify to be treated by law as reasonably well informed subjects.

Similarly, the role entrusted to information in EU personal data protection law and in EU consumer law is appreciably different: whereas for the latter it can facilitate ma-

89 Para 48.

90 Specifically, Art. 12(2) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002, 37-47.

91 Para 62.

92 Idem.

93 Case C-49/11, *Content Services Ltd v Bundesarbeitskammer*, 5 July 2012, para 37.

king choices between products and services, for the former it has instead other purposes (namely, contributing to fair and transparent processing, and allowing for consent). It is somehow delicate, thus, to attempt to expand on the conception of the data subject as consumer in order to configure information obligations imposed on data controllers as helping to make choices between different data processing practices.[94]

There are, however, also dimensions of personal data protection law that could benefit from taking into account the way in which EU law conceptualises consumers. One of them is the construal of vulnerability: it is not limited to children, but can be recognised as affecting also other groups, and is in any case something different than a mere (temporary) unawareness of risks, which is what the European Commission is habitually identifying as affecting children.

More importantly, defining a standard notion of data subject in terms of information and capability to make choices appears as a necessary prerequisite to define which online practices are unlawfully misleading. It is striking that despite the significance of the data subject's right to know and of information obligations imposed on data controllers for European personal data protection, there is no clear benchmark in EU law as to the level of misinformation of data subjects to be regarded as unlawful. The current stress on the need for information provided by data controllers to be 'transparent' is based on the concession that the instruments typically presented as supposedly complying with the data controllers' duty to inform (the 'privacy policies' or 'privacy notices' proliferating online) are commonly uninformative. In defiance of this contention, however, the legislator does not appear to be ready to directly qualify uninformative and deceptive so-called 'privacy' tools as unlawful, or to provide clearer specifications as to what is always to be regarded as un-transparent and unfair.

4. CONCLUDING REMARKS

This contribution has examined the relationship between information and the protection of individuals from the perspective of EU personal data protection. It has identified the existence of a kind of structural ignorance that is ascribed to the data subject, partially mitigated through the imposition of information obligations on data controllers. The recently re-invented notion of transparency as a set of formal demands applicable to information obligations confirms their importance in the building up of EU personal data protection. Together with this approach, the idea that data subjects shall be protected as unaware consumers of not free online services is gaining momentum.

94 Which is the path followed by the EDPS in European Data Protection Supervisor (EDPS) (2014), op. cit (see notably p. 34).

Data subjects are more than consumers. They are the individuals to whom is granted the EU fundamental right to the protection of personal data, and the EU is responsible to respect and promote its fundamental rights. As described, the right to personal data protection brings about the need to inform individuals about what happens to their personal data, but also about the existence of their subjective rights, and, possibly, about the risks or consequences of consenting or refusing to consent to some data processing practices.

In reality, the active exercise of this right by individuals might actually require not only the existence of a certain right to know, but also an awareness of the limitations of the information they are legally entitled to receive, as an open invitation to act very observantly and with circumspection even in the absence of satisfactory levels of information –or precisely because of such absence. Perhaps data subjects able to make better decisions online are not data subjects surrounded by more transparent 'privacy' notices, but data subjects more acutely aware of the fragility of the knowledge at their disposal.

5. BIBLIOGRAPHY

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce, New York, May 17 - 20, 2004*, 21-29, doi>10.1145/988772.988777.

Brandimarte, L., Acquisti A. and Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* (4) 340, DOI: 10.1177/1948550612455931.

Bygrave, L. A. (2002). *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

European Data Protection Supervisor (EDPS) (2014). *Preliminary Opinion of the EDPS: Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, March.

González Vaqué, L. (2005). La noción de consumidor en el Derecho comunitario del consumo. *Estudios sobre consumo*, *75,* 25-42.

Hildebrandt, M. and Koops, B. J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *The Modern Law Review, 73 (3*), 428-460.

Incardona R. and Poncibò, C. (2007). The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution. *J Consum Policy 30*, 21–38.

Kuczerawy, A. and Coudert, F. (2011). Privacy Settings in Social Networking Sites: Is It Fair? In Simone Fisher-Hübner et al. (eds.), *Privacy and Identity Management for Life*, International Federation for Information Processing (IFIP), 231-243.

MacMaoláin, C. (2007). EU Food Law: Protecting Consumers and Health in a Common Market, Oxford: Hart Publishing,

Robinson, N. et al. (2009), *Review of the European Data Protection Directive*, RAND Europe.

Ruiz, M. C. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo, 7(14),* 7-43.

Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers and the Rights of Citizens*, 1973.

Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. 126 *Harvard Law Review* 1880; GWU Legal Studies Research Paper No. 2012-141.

Van Alsenoy, B. (2012). *D6.1: Legal Requirements for Privacy-Friendly Model Privacy Policies*. Security and Privacy in Online Social Networks (SPION).

Van der Meulen, B. and Van der Velde, M. (2011). *European Food Law Handbook*. The Netherlands: Wageningen Academic Publishers.

Wauters, E., Lievens, E. and Valcke, P. (2013). *D1.2.4: A Legal Analysis of Terms of Use of Social*

Networking Sites, Including a Practical Legal Guide for Users: Rights & Obligations in a Social Media Environment.

Westin, A. F. (1970, originally published in 1967). *Privacy and Freedom.* New York: Atheneum.

Whitman, J Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal, 113,* 1151-1221.

RESPONSABILIDAD CIVIL POR LA INCLUSIÓN DE DATOS PERSONALES EN UN FICHERO DE SOLVENCIA PATRIMONIAL

Albert Ruda González
Prof. agregado de Derecho Civil de la Universitat de Girona

Natalia Wilson Aponte
Becaria predoctoral de la Universitat de Girona

RESUMEN: La ley española permite que los datos de los morosos se inscriban en ficheros de solvencia patrimonial. Sin embargo, la inclusión indebida de esos datos puede ocasionar daños por los que hay que responder civilmente. Se examinan las líneas generales de este supuesto de responsabilidad en el Derecho español.

PALABRAS CLAVE: Datos personales, ficheros, solvencia, morosos, responsabilidad.

1. INTRODUCCIÓN

Como es sabido, nuestra legislación permite que existan ficheros de solvencia patrimonial, popularmente llamados «ficheros de morosos». Dichos ficheros cumplen una determinada función, en tanto que informan a operadores en el mercado sobre la posible solvencia de una determinada persona, conforme a la ley. No obstante, la inclusión errónea o incorrecta en ese tipo de ficheros, sea por suplantación de identidad u otro motivo, puede causar distintos daños a la persona en cuestión, que afecten a su interés en la protección de datos personales, o a sus derecho a la intimidad o el honor, entre otros. Este trabajo expone de modo sucinto la situación de dichos ficheros conforme a la legislación española y, en especial, la responsabilidad extracontractual por daños causados por la inclusión indebida en los mismos, a la luz de la jurisprudencia del Tribunal Supremo.

Lógicamente, por razones de espacio resulta imposible en un trabajo de estas características ofrecer una visión global de todos los aspectos jurídicos relacionados con el tratamiento de datos de solvencia en general, y de los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias en particular. En este breve estudio solo se pretende aproximarse a un aspecto concreto, como es la responsabilidad extracontractual o civil derivada de la inclusión indebida en esos ficheros. Ahora bien, parece claro que este extremo no puede abordarse sin detenerse antes, aunque sea de modo sucinto, en el marco legislativo que regula las condiciones del tratamiento y las garantías de los titulares de los datos. Dicho marco, como es natural, establece buena

parte de los parámetros a tener en cuenta a la hora de examinar la cuestión de la responsabilidad. Además, hay que tomar en consideración la manera en que la jurisprudencia se ha enfrentado a la misma. En concreto, ya existe una buena serie de sentencias sobre la indemnización de daños por un tratamiento indebido de datos por los ficheros de morosos. A ese material legal y jurisprudencial hay que añadir la interpretación adoptada por la doctrina científica, cuya atención creciente a estos problemas ha ido a la par con el aumento de reclamaciones ante los juzgados por asuntos de este tipo. Todos esos materiales permiten definir el régimen específico de los ficheros de morosos, al que se hará alusión más abajo.

De acuerdo con lo anterior, este trabajo describe brevemente los ficheros de solvencia patrimonial, su función y funcionamiento; los requisitos para que los datos de una persona se inscriban en ellos, así como el tratamiento que deben recibir, y la responsabilidad causada por un tratamiento indebido, incorrecto o inexacto. Así pues, se trata de exponer cómo se pueden producir daños en este ámbito, además de las consecuencias jurídicas que el incumplimiento de los requisitos que se expongan en la primera parte del trabajo produce en el orden jurídico-civil. Se dedicará especial énfasis a los casos consistentes en intromisiones ilegítimas al derecho al honor, dado que, como se puede anticipar, han centrado el debate jurídico en los tribunales. A este respecto, habrá que analizar la conducta desplegada tanto por el responsable del tratamiento como por el titular del fichero, con el objeto de determinar si se enfrentan a una posible responsabilidad civil y, en caso afirmativo, las circunstancias y límites de su configuración.

Finalmente, se hará referencia a algunos criterios para determinar el monto de las indemnizaciones por los daños causados en virtud de la inclusión indebida en el fichero de morosos.

2. FUNCIÓN DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL

La primera cuestión que se podría plantear en relación con el tema objeto de este estudio es el de la función de los ficheros de solvencia patrimonial. Si estos ficheros producen daños, una pregunta casi obvia consistiría en porqué no suprimirlos o prohibirlos. No obstante, existen buenas razones para no seguir una opción tan radical.

Para comenzar, resulta evidente que no todas las actividades potencialmente dañosas deben prohibirse. Actividades susceptibles de generar daños también producen efectos socialmente deseables. En realidad, existen razones de peso que explican la existencia y el funcionamiento de los ficheros de solvencia patrimonial. Esos ficheros cumplen fundamentalmente una función de información a favor de terceros.[1] Son, en cierto

1 Hualde Manso, T. (2013). Ficheros de morosos, nulidad del Reglamento de Protección de Datos y Derecho al Honor. *Revista Doctrinal Aranzadi Civil-Mercantil* (8), 49.

modo, similares a otros tipos de Registro, como el de la propiedad (RP), en la medida en que ofrecen a terceros interesados datos relevantes sobre determinadas personas, en su dimensión patrimonial. De modo análogo al potencial concedente de un crédito, que quiere informarse sobre qué activos inmobiliarios constan inscritos en el RP a favor del solicitante de aquel, otros agentes económicos pueden acceder a información sobre la solvencia de las personas inscritas mediante la consulta de los ficheros de morosos. Mediante esa información se pretende dar razón, con cierto nivel de veracidad, del grado de cumplimiento de sus obligaciones por parte de las personas que han desarrollado alguna actividad en el tráfico económico. Por tanto, el comúnmente llamado fichero de morosos es de gran utilidad para quienes se encuentran en condiciones de contratar en la medida que les interesa conocer la situación económica de su eventual co-contratante.[2]

Especificamente respecto a los ficheros de solvencia y crédito, como sistemas de intercambio de información entre entidades financieras sobre la solvencia de los clientes, su finalidad es poner a disposición de esas entidades datos sobre los potenciales prestatarios en lo que atañe a la forma en la cual han satisfecho sus deudas: falta de pago, avales o fianzas, etc. Asimismo, dichos ficheros despliegan efectos globales positivos, en tanto que contribuyen a reducir el incumplimiento de los prestatarios, a prevenir el endeudamiento excesivo y, paralelamente, a generar mayor disponibildad de crédito. Nuevamente, el paralelismo con el RP es claro, dado que también es comúnmente reconocido que facilita el tráfico económico al proporcionar seguridad. Los órganos de justicia se han hecho eco de las virtudes del sistema de información articulado mediante los ficheros de morosos. Incluso el Tribunal de Justicia de la Comunidad Europea ha reconocido los efectos positivos de los mismos cuando ha examinado cuestiones relativas a la protección de datos personales.[3]

Desde un punto de vista de política jurídica, parece claro que los ficheros de morosos, en la medida en que informan de la solvencia económica de las personas, son perfectamente legítimos. Su función, en este sentido, es de desarrollo de funciones de saneamiento y clarificación del tráfico económico.[4] Tanto más en situaciones en las cuales el mercado de la intermediación financiera se ve afectado por el aumento del índice de morosidad, como sucede en el contexto actual, en que ha alcanzado máximos históricos.[5]

---

2 Pérez de Ontiveros, C. (2012). Ficheros de solvencia patrimonial y de crédito: Cuestiones civiles y su apreciación por los tribunales del orden Contencioso-Administrativo. *Revista Aranzadi de Derecho Patrimonial* (28), 148.

3 STJCE (3) de 23.11.2006 (Asunto C-238/2005), apartados 46, 55, 67 y 71

4 Entre otros, Parra Lucán, M. (2011). Registro de morosos: Derecho civil y nulidad (parcial) del reglamento de desarrollo de la Ley Orgánica de protección de datos. *Revista Aranzadi Civil Doctrinal* (3), 83.

5 En diciembre de 2013 la morosidad de la banca española aumentó hasta el 13,6%, según datos de El País (http://economia.elpais.com/economia/2014/02/18/actualidad/1392714550_402874.html).

Un contexto como el actual favorece que los acreedores en conjunto sientan la necesidad de tomar medidas que les permitan acceder a suficiente información con base en la cual decidan otorgar o negar créditos de manera responsable. Por tanto, es necesario para ellos valorar fidedignamente las circunstancias específicas de cada solicitante de un crédito, por ejemplo.[6]

Sin embargo, el cumplimiento de las finalidades referidas debe verse a la luz del uso dado a tales registros. No cabe duda de que la efectiva generación o no de esos efectos positivos depende del modo en el cual estos sean utilizados. La teórica bondad del instrumento serviría de poco si en la práctica se convirtiesen en un mecanismo de abuso. Por ende, si los registros se manejasen como un arma impuesta por una de las partes de la contratación, no solo se atentaría contra la existencia y conservación del mercado en términos de competencia sino que adicionalmente se podrían vulnerar derechos fundamentales y de la personalidad del individuo en cuestión. En esta línea, el Tribunal de Defensa de la Competencia (TDC) ha subrayado que no debe ser admitido el registro en el fichero de morosos si se emplea como un instrumento para responder colectivamente con la explusión de un sujeto del mercado o para impedir su reingreso.[7] Dicha conducta atenta flagrantemente contra la existencia y conservación del mercado del que se trate.

Los tribunales españoles han señalado con buen criterio que el fichero de morosos, cuando se convierte en un método de presión, puede constituir una intromisión ilegítima en el derecho al honor. Así sucede cuando es usado por las grandes empresas para obtener el pago de las sumas que consideran debidas, valiéndose del temor al descrédito personal, el menoscabo del prestigio profesional o la denegación de créditos que conlleva aparecer en tales ficheros (en esta línea, véase la STS (1ª) de 6.3.2013 [Roj STS 1715/2013]). La intromisión obedece precisamente al desvalor social que significa aparecer como deudor moroso sin serlo en realidad. La inclusión de morosos en los ficheros de solvencia económica así configurada, además de apartarse de su objetivo principal, se convierte en abusiva y desproporcionada.

A ese potencial de mal uso se añade otro inconveniente, cual es la desigualdad que la mera existencia de los ficheros de morosos produce entre los operadores económicos implicados. En efecto, esos ficheros pueden calificarse con razón de asimétricos, básicamente por dos razones. La primera tiene que ver con la información que contienen, en tanto que solo se limitan a indicar la identidad del deudor, la identidad del acreedor, el número y la cuantía de la deuda, pero no prevén la procedencia u origen de la misma. Para ello habría que hacer constar, además, la información que convenga sobre el contratro u otra fuente de la obligación que se considera incumplida (por ejemplo, si se

6 Resolución del Tribunal de Defensa de la Competencia de 18.9.1992 (Resolución 33/92), apartado 5º

7 Véase la nota anterior.

trata de un contrato de seguro vinculado a una hipoteca). La segunda razón se relaciona con la inexistencia de un fichero de información que identifique a las entidades que no cumplen sus obligaciones frente a sus clientes.[8] De este modo, los clientes no pueden acceder a un fichero en el que por ejemplo se reflejen los incumplimientos de las entidades de crédito. La desigualdad de armas salta a la vista.

Para evitar incurrir en prácticas lesivas como la inclusión indebida de una persona en un fichero de este tipo, es indispensable que el uso de los registros de morosos y el tratamiento dado a los datos que allí se almacenan se lleve a cabo dentro de los parámetros legales y jurisprudenciales que protegen los derechos y garantías de los titulares de los datos. Se van a examinar a continuación.

3. REQUISITOS PARA UN TRATAMIENTO ADECUADO DE DATOS SOBRE SOLVENCIA PATRIMONIAL

Como es sabido, ha sido el legislador comunitario europeo el que ha establecido la base sobre la cual debe realizarse el tratamiento de los datos de morosidad. En concreto, la Directiva 1995/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,[9] permite de forma restrictiva tomar decisiones individuales automatizadas con efectos jurídicos respecto a algún aspecto de la personalidad de un sujeto, tal como sería su rendimiento crediticio, en dos eventos: i) cuando se hayan adoptado en virtud de un contrato cuya petición de celebración o ejecución por el interesado haya sido satisfecha o existan las medidas apropiadas para salvaguardar su interés legítimo, o ii) cuando estén autorizadas por una ley que garantice ese interés legítimo (art. 15).

Siguiendo esa orientación, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD),[10] reguló específicamente la prestación de servicios de información sobre solvencia patrimonial y de crédito para garantizar la protección del interés legítimo referido (art. 29). Igualmente, el Real Decreto 1720/2007,[11] mediante el cual se desarrolla dicha Ley, contiene las disposiciones aplicables a los fiche-

8 Hualde, cit., 52.

9 Directiva 1995/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos(DOCEL L, núm. 281, 23.11.1994, pág. 31-50).

10 BOE núm. 298, de 14.12.1999.

11 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17, de 19.01.2008).

ros de información sobre solvencia patrimonial y de crédito (arts. 37-44). Dicho Reglamento, a su vez, ha sido objeto de pronunciamientos por parte del Tribunal Supremo, quien ha declarado la nulidad parcial de varios de sus preceptos.[12] En concreto, la norma reglamentaria no cumplía con los mínimos de concreción que, a juicio del TS, impone la legislación actual (art. 4.3 LOPD).[13] Se trata, pues, de una materia controvertida, como salta a la vista, en la que algunos pasos dados por el regulador han tenido que ser desactivados por los tribunales de justicia.

Adicionalmente, la Agencia Española de Protección de Datos emitió, en el ejercicio de la facultad normativa que la ley le atribuye (art. 37.1.c) LOPD), una norma específica sobre este tipo de ficheros, a saber, la Instrucción 1/1995.[14] Precisa el tratamiento de datos de carácter personal relativos al cumplimiento e incumplimiento de obligaciones dinerarias dentro del marco de la prestación de servicios de información sobre solvencia patrimonial y crédito.

Por su parte, la jurisprudencia ha desplegado una labor crucial, como se va a ver, para poder adaptar las normas mencionadas a los casos contretos, o al revés, subsumir dichos casos en el marco legal, con la pretensión principal de salvaguardar los intereses legítimos de los titulares de los datos objeto del tratamiento referido.

Pues bien, habiendo pasado revista rápidamente al marco normativo dentro del cual se establecen las condiciones para llevar a cabo un tratamiento adecuado de datos sobre solvencia patrimonial, a continuación se analizarán cada uno de los requisitos que son exigidos a estos efectos.

3.1. Fuente de procedencia de los datos

El artículo 29 de la LOPD, refiriéndose a los prestadores de servicios de información sobre solvencia patrimonial y crédito, plantea los siguientes dos escenarios. En primer lugar, se encuentran los ficheros limitados a tratar datos de carácter personal a partir de los registros y de las fuentes accesibles al público o suministrados directamente del titular del dato o con su consentimiento. El segundo escenario es el referente a los casos en que los prestadores de ese servicio recaban, del acreedor o de quien actúe por su cuenta o interés, datos sobre el cumplimiento o incumplimiento de obligaciones dinerarias por parte de otra persona.

---

12 STS (3ª) de 15.7.2010 (Roj STS 4047/2010; Roj STS 4050/2010; Roj STS 4057/2010).

13 Críticamente, puede verse sobre este extremo Linares Gutiérrez, A. (2011). La inclusión de datos en ficheros sobre solvencia patrimonial: cuestiones controvertidas. Crítica a la Sentencia del Tribunal Supremo de 15 de julio de 2010. *Dereito* (21), 217.232 <http://www.usc.es/revistas/index.php/dereito/article/view/830/805> (consultado: 10.3.2014), 219 ss.

14 Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito (BOE núm. 54, de 4.3.1995).

Como se desprende de dicho precepto, se trata de dos tipos de ficheros con características diferentes. En el primer caso nos encontramos ante ficheros de datos positivos o de solvencia patrimonial, que no se apartan de la regulación común que establece la LOPD. Esos ficheros pretenden ofrecer una imagen veraz de la solvencia de las personas, con el historial de cumplimiento de sus obligaciones, el uso de tarjetas de crédito sin problemas y los niveles de endeudamiento global de los consumidores. En cambio, en el segundo caso el escenario tiene que ver con los ficheros negativos o de incumplimiento de obligaciones pecuniarias, conocidos como ficheros de morosos o de morosidad. Lógicamente, son los ficheros pertenecientes a este segundo grupo los que, dadas sus características, exigen un tratamiento más cuidadoso y garantista frente a los intereses de los presuntos deudores, pues son estos ficheros los que publican un perfil desfavorable de la persona.[15]

En este segundo escenario el acreedor o quien actúe por su cuenta o interés será entonces quien ceda los datos de la deuda al fichero común, incluso sin el consentimiento del afectado o en contra de su voluntad. No obstante, el afectado deberá ser notificado de los datos incluidos en el fichero de morosos, así como de su derecho a recabar información de la totalidad de tales datos, en un plazo de treinta días desde dicho registro (art. 29.2 LOPD).

3.2. Calidad de los datos

Cuestión distinta de la anterior es la de la calidad de los datos. Con carácter general consiste en garantizar que la recolección y tratamiento se realice sobre datos adecuados, pertinentes, exactos y no excesivos con respecto a las finalidades explícitas y legítimas de su obtención (art. 4 LOPD).

Ahora bien, en relación con los datos registrables en los ficheros de solvencia, la LOPD solo establece que estos deben ser determinantes para enjuiciar la solvencia económica de los interesados y que no deben referirse, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a su situación actual (art. 29.4). Es evidente la falta de coincidencia entre ese plazo y el general de prescripción de las acciones personales, de quince años (art. 1964 CC). La discordancia puede explicarse tal vez por la intención legal de proteger el derecho al olvido, por un lado, y la existencia de una autoridad administrativa que vela por el cumplimiento de la normativa específica, cual es la Agencia de protección de datos (o equivalente territorial).[16]

---

15 Entre otros, puede verse Cuena Casas, M. (2014). Préstamo responsable, información crediticia y protección de datos personales. Revista de derecho concursal y paraconcursal (20), 161-185, también disponible en <http://www.elnotario.es/images/pdf/PRESTAMO_RESPONSABLE.pdf> (consultado: 10.3.2014), 17.

16 Parecidamente, véase Parra, cit., 91.

Por su parte, el RD 1720/2007 y la Instrucción 1/1995 adecuan especificamente ese requisito a los datos relativos al cumplimiento e incumplimiento de obligaciones dinerarias. Condicionan así la cesión de estos datos a la existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada (art. 38.1 RD 1720/2007, y Norma 1 de la Instrucción 1/1995).

Tanto la jurisprudencia como la doctrina se han pronunciado sobre el cumplimiento de los anteriores requisitos. Se ha discutido con especial detenimiento lo que debe entenderse por deuda cierta, en tanto que las dudas acerca de la existencia de la deuda impedirían su inclusión en el fichero de morosos. Es decir, no sólo la inclusión de deudas inexistentes atentan contra el principio de calidad de los datos, también lo hace la inclusión de deudas controvertidas.

En el primer caso, por ejemplo, con ocasión de la inclusión errónea de una deuda no exigible a la recurrente –por inexistencia del contrato de crédito–, la Sala Civil del Tribunal Supremo (TS) señaló que comunicar hechos no veraces es una conducta contraria a los buenos usos y prácticas bancarias, máxime si se trata de imputar falsamente a alguien la condición de moroso en la medida que constituye una intromisión en el derecho al honor, afecta el prestigio personal y profesional causando daños de tipo moral (STS [1ª] de 9.4.2012 [Roj STS 2638/2012]).

La inclusión de deudas de veracidad dudosa y de existencia controvertida también vulnera el principio de calidad de los datos y, paralelamente, también puede constituir una intromisión en el derecho al honor. El mismo Tribunal se pronunció en ese sentido en un caso en el cual la deuda imputada al supuesto moroso tenía origen en unos contratos vinculados, siendo así que se había extinguido el contrato principal (STS [1ª] de 6.3.2013 [Roj STS 1715/2013]). El TS afirmó entonces que, cancelada la operación principal –correspondiente a un préstamo hipotecario– «subsiste cuando menos la duda de si debían considerarse subsistentes los demás». En otras palabras, la extinción del contrato principal cierne una duda sobre la subsistencia del contrato vinculado al anterior.

Por otra parte, a partir de la ya referida nulidad parcial del art. 38.1 del RD 1720/2007 (decretada por la antes citada STS [3ª] de 15.7.2010 por falta de concreción), la presentación de la reclamación judicial, arbitral o administrativa por parte del afectado no impide por sí sola la inclusión de datos en el fichero.

Antes de la anulación parcial de la norma referida, además de requerir la existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada, el reglamento en cuestión establecía que respecto de esa deuda no se hubiese *entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero*.

Actualmente se ha entendido que si se presentan reclamaciones como las descritas en el párrafo anterior, permitirían cuestionar la certeza de la deuda y solicitar la cance-

lación del dato incluido en el fichero. No obstante, si este no es cancelado y finalmente se emite resolución declarando la inexistencia de la deuda, dicha resolución generará efectos *ex tunc*.[17]

Igualmente, en la misma actuación, se decretó la nulidad del apartado 2 de la norma arriba señalada. Concretamente, el art. 38.2 impedía incluir en los ficheros datos sobre los que existiese *un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores (…),* refiriéndose a la deuda cierta, vencida, exigible, que haya resultado impagada. *Sin embargo, para esos efectos sí es admisible el principio de prueba documental conforme a la Instrucción 1/1995 antes mencionada.*

Finalmente, con el objeto de determinar el cumplimiento del principio de calidad en cada caso concreto, el acreedor o quien actúe por su cuenta o interés deberá asegurarse de que concurren todos los requisitos exigidos. De lo contrario, podría verse sancionado administrativamente y, en caso de causar daños sean morales o patrimoniales, al pago de una indemnización.

Así, por ejemplo, la Audiencia Nacional emitió un fallo mediante el cual sancionó a una empresa distribuidora que realizó un tratamiento indebido de datos por el impago de mensualidades causadas en una supuesta contratación de servicios (Sentencia de la Audiencia Nacional [SAN] de 29.1.2014 [Roj SAN 175/2014]). La sentencia afirma que la empresa, como responsable del tratamiento de datos, tiene un deber especial de diligencia cuya intensidad se encuentra potenciada por la relevancia de los bienes jurídicos protegidos y por la profesionalidad de la empresa misma, más aun cuando opera con ánimo de lucro.

De igual forma, en otro caso parecido la sala de lo Contencioso del TS consideró que el error en el tratamiento de datos se produjo por falta de diligencia de la entidad sancionada en tanto que fue la configuración del sistema informático la que originó la inclusión del recurrente en el fichero (STS [3ª] de 23.1.2007 [Roj STS 224/2007]). El Alto Tribunal destacó la especial sensibilidad de los bienes jurídicos en juego, los cuales a su vez hacen exigible una especial diligencia por parte de las entidades que se benefician de dicho tratamiento y afirmó que estas últimas deben prever ese tipo de inconsistencias, sin perjuicio del grado de intencionalidad en la conducta a los efectos de graduar la sanción correspondiente conforme a la ley.

En conclusión, considerando que el artículo 18.4 de la Constitución le reconoce a cada persona un poder de disposición y de control sobre sus datos, se deriva de todo lo anterior que es necesario extremar las exigencias respecto a la calidad de estos, sobre todo si se tiene en cuenta que la inclusión de los datos en los ficheros de morosos se hace sin contar con el consentimiento de sus titulares y con la posibilidad de atentar contra derechos fundamentales como el honor (en esta línea, STS [1ª] de 22.1.2014 [Roj STS 355/2014]).

17 Entre otros, Mendoza Losana, A. (2012). Guía práctica sobre la inclusión en un registro de morosos. *Revista CESCO de Derecho de Consumo* (4), 151.

3.3. Actualidad de los datos

Los datos incluidos en el fichero tienen que ser «actuales». La palabra entrecomillada tiene un sentido amplio, ya que los datos que se incluyan en los ficheros de morosos no deben referirse a más de seis años. Es decir, no debe haber transcurrido dicho lapso de tiempo desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si fuera de vencimiento periódico (art. 38.1.b) RD 1720/2007).

Por lo tanto, el pago de la deuda registrada en el fichero de morosos da lugar a su cancelación de forma inmediata (art. 41 RD 1720/2007).

3.4. Previo requerimiento de pago

Antes de realizar la cesión de datos sobre la deuda al fichero de morosos, es indispensable requerir al afectado para que pague (art. 38.1.c) RD 1720/2007 y Norma 1 de la Instrucción 1/1995).

En dicha comunicación deberá advertirse que, si no se produce el pago solicitado, sus datos podrán ser comunicados a los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias (art. 39 RD 1720/2007).

En caso que efectivamente exista una deuda, si no se presenta el requerimiento de pago con las condiciones descritas, el acreedor podría resultar obligado a indemnizar los daños que se hayan derivado de la inclusión en los referidos ficheros. Así se deriva de una sentencia de la Audiencia Provincial de Segovia, conforme a la cual la responsabilidad civil derivada del artículo 23 de la Directiva 95/46 y de la LOPD 15/1999, es objetiva (SAP Segovia de 25.4.2002 [JUR 2002/185043]).

En caso de que el afectado niegue haber sido notificado de este requerimiento, le corresponderá al acreedor demostrar lo contrario –como se desprende de la práctica judicial. En particular, el Tribunal Supremo ha entendido que no se exige a efectos procesales que el requerimiento de pago se lleve a cabo de forma fehaciente. Así lo afirmó en un caso en el que la entidad crediticia, una vez vencida la obligación, había requerido el pago a los demandados con la advertencia de incluirlos, en el supuesto de impago, en el fichero de morosos (STS [1ª] de 9.1.2013 [Roj STS 545/2013]).

4. INCUMPLIMIENTO DE LOS REQUISITOS DEL TRATAMIENTO DE DATOS SOBRE SOLVENCIA PATRIMONIAL

El incumplimiento de los requisitos señalados y, en general, las actuaciones contrarias a las normas de protección de datos, pueden dar lugar a procesos independientes de responsabilidad tanto administrativa (es decir, frente a la Administración pública) como civil. La existencia de diferentes mecanismos de tutela a favor del afectado no implica

subordinación de uno de estos mecanismos respecto del otro. Más bien pueden ponerse en funcionamiento incluso de forma coetánea.

La LOPD dispone que el responsable del fichero o tratamiento es la persona física o jurídica, de naturaleza pública o privada que decide sobre la finalidad, el contenido y el uso del tratamiento. El encargado del tratamiento por su parte, es quien trata datos personales por cuenta del primero, es decir, por cuenta del responsable (art. 3.d) y g)). Ahora bien, para garantizar la observancia de los requisitos mencionados, dichos sujetos deben cumplir con ciertos deberes legales según la fase del tratamiento en cuestión. Por ejemplo, tal como se ha señalado, antes de incluir en el registro los datos crediticios del afectado, el acreedor (responsable del tratamiento) deberá informarle sobre la inclusión. Asimismo, una vez realizado el registro, el responsable del fichero deberá efectuar la notificación correspondiente.

A su vez, la LOPD faculta a los afectados a ejercer los derechos de acceso, rectificación, cancelación y oposición ante el titular del fichero, ante el responsable del tratamiento o ante cualquier otra entidad. En caso de su denegación, podrá acudir a la Agencia de Protección de Datos o al organismo competente en cada Comunidad Autonómica para que se pronuncie sobre la procedencia o improcedencia de dicha denegación (arts. 14-18 LOPD y art. 44 RD 1720/2007).

Adicionalmente, la LOPD le reconoce al afectado el derecho a obtener la debida indemnización por el daño o lesión sufrida como consecuencia del incumplimiento de la Ley (art. 19). Sobre este deber de indemnizar se hablará más adelante.

En el caso del procedimiento administrativo, la norma le atribuye a la Agencia de Protección de Datos la facultad sancionadora para la represión de las conductas contrarias a la Ley. La Agencia deberá emitir una resolución expresa de tutela de derechos, circunscribiendo su análisis a los ilícitos administrativos previstos legalmente. No obstante, en la práctica no siempre resulta tarea fácil delimitar esa función, sobre todo cuando se trata de conflictos que deben ser resueltos por los tribunales civiles, como es el caso de decidir si una deuda es cierta o no o si existía un contrato entre las partes.[18]

En cuanto a la imputación de la sanción, es importante determinar en cada caso concreto el papel que desempeñan los sujetos involucrados en el tratamiento de datos, en la medida que, tal como normalmente lo indica el TS en sus sentencias, no cabe extender este régimen a cualquier persona so pena de incurrir en una aplicación extensiva o analógica de las sanciones (STS [3ª] de 29.7.2002 [Roj STS 5753/2002]). Ahora bien, a partir de la LOPD no solo el responsable del fichero puede verse sancionado por incumplir la ley. El acreedor responsable del tratamiento o quien actúe por su cuenta o interés, al ser quien decide sobre la finalidad, contenido y uso de los datos, también se considera responsable. Ese acreedor responde específicamente ante la inexactitud o inexistencia de

18 Véase, Parra, cit., 93-94.

los datos que hubiera facilitado para su inclusión en el fichero (art. 43 RD 1720/2007). En todo caso, contra la resolución que emita la Agencia de Protección de Datos procede recurso contencioso-administrativo.

5. RESPONSABILIDAD CIVIL POR LOS DAÑOS CAUSADOS A PARTIR DE LA INCLUSIÓN INDEBIDA DE DATOS EN EL FICHERO DE MOROSOS

En lo que se respecta a la responsabilidad extracontractual o civil, como se verá más abajo, el daño o perjuicio generado por el incumplimiento de la Ley da lugar a indemnizar al afectado. Si se trata de ficheros de titularidad pública, se exigirá responsabilidad conforme al régimen jurídico especial de las Administraciones públicas (art. 139 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).[19] Tratándose de ficheros de titularidad privada, se ejercitará la correspondiente acción ante la jurisdicción ordinaria (art. 19 LOPD). La responsabilidad puede ser de tipo contractual (sujeta al régimen de los arts. 1101 ss. del Código Civil español [CC]), cuando supone el incumplimiento del acuerdo entre las partes, o extracontractual en otro caso.[20]

Pues bien, pese a que el artículo 19 LOPD reconoce expresamente el derecho a la indemnización, es una norma insuficiente para ser aplicada directamente con esa pretensión. Efectivamente, nada dice sobre el tipo de responsabilidad, el daño que se genera, los criterios para su valoración, entre otros. Por tanto, dependiento del asunto de que se trate, es necesario acudir a las normas especiales que regulan el supuesto que se está estudiando aquí o, en su defecto, adaptar las normas generales sobre responsabilidad civil (en el caso de la extracontractual, se trataría, como es sabido, del art. 1902 y ss. CC).

Es decir, el tratamiento indebido de datos –que por sí mismo vulnera el derecho fundamental a la protección de datos personales– podría encontrarse asociado a la vulneración de otros derechos. En lo que atañe a la inclusión errónea de de datos personales en ficheros de morosos, esa vulneración podría traducirse en una intromisión ilegítima al derecho al honor, evento que encuentra su marco regulatorio en una norma específica de protección: la Ley Orgánica 1/1982, de 5 de mayo, de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.[21]

---

19 BOE núm. 285, de 27.11.1992.

20 Por todos, Plaza Penadés, J. (2013), Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en Internet, en: Plaza Penadés, J. (dir.), *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur menor: Thomson Reuters Aranzadi, 1133-1174, 1146 n. 8.

21 BOE núm. 115, de 14.5.1982.

A partir de la decisiva STS (1ª) de 24.4.2009 (RJ 2009/3166), se estableció como criterio que la inclusión errónea en un registro de morosos sin que se cumpla el requisito (antes referido) de veracidad se constituye en una intromisión ilegítima en el derecho al honor. El Tribunal Supremo expone a estos efectos que imputar la condición de moroso a una persona que no lo es atenta contra su dignidad. En efecto, dicha conducta resulta ser lesiva en dos sentidos: i) atenta contra la propia estima del afectado, y ii) menoscaba su fama ante los demás. Por consiguiente, es intrascendente que esa falsa morosidad haya sido o no conocida por por terceras personas mediante la consulta del fichero de morosos. Basta con posibilitar su conocimiento al público, con la mera cognoscibilidad, para que la intromisión se produzca.

En estos eventos, en los que está en juego uno de los derechos de la personalidad, se aplicará el régimen de responsabilidad contenido en la norma especial que lo regula. Así, conforme a la LO 1/1982, acreditada la intromisión ilegítima en el derecho al honor se presume el perjuicio, cuya indemnización se extiende al daño moral (art. 9.3).

Tal como lo reconoce el Tribunal, esta presunción opera *iuris et de iure* (STS [1ª] de 22.1.2014, ya citada). En este caso la presunción se presenta con ocasión del tratamiento de datos personales en un registro de morosos sin cumplir las exigencias que establece la LOPD. La indemnización del daño moral corresponderá a la afectación a la dignidad en su aspecto subjetivo o interno (afectación del interesado) y objetivo o externo (consideración de las demás personas). Este último dependerá de la divulgación y consulta de la información. En el caso de la sentencia citada, el Tribunal también reconoció que «sería indemnizable el quebranto y la angustia producida por el proceso más o menos complicado que haya tenido que seguir el afectado para la rectificación o cancelación de los datos incorrectamente tratados».

Ello no quiere decir que la difusión de los datos del fichero de morosos sea irrelevante, antes lo contrario. Si el registro es efectivamente consultado por terceras personas, esa circunstancia será tenida en cuenta, dado que puede producir nuevos daños, o agravar los existentes. Por ejemplo, el daño moral consistente en la mera inclusión puede sumarse a un daño derivado de la denegación de un préstamo hipotecario, o el rechazo de una línea de crédito.[22] En otro caso, podría agravarse el daño moral ya producido, lo cual tendría su repercusión en el momento de determinar el monto de la indemnización. Por ejemplo: a partir de la inclusión errónea, un comerciante podría verse afectado económicamente por un rechazo al acceso a una línea crediticia, pero también sufrir un quebranto moral mayor por el hecho de saber que en su entorno personal y familiar se ha conocido su morosidad. La «difusión o audiencia del medio» de la lesión al honor es uno de los criterios tenidos en cuenta por la LO 1/1982 (art. 9.3). De hecho, incluso

22 Véase el caso comentado por Rubio Torrano, E. (2012). Inclusión indebida en fichero de morosos. Intromisión ilegítima en el derecho al honor. *Revista Aranzadi Civil-Mercantil* (7), 91-95.

cabría preguntarse si cabe reclamar el lucro obtenido, en su caso, por la intromisión (art. 9.2.d).

Lo anterior permite plantear si es posible exigir indemnización diferenciada tanto por la intromisión al honor como por la vulneración a la LOPD cuando se produce un daño, cuestión que se examina a continuación.

Como se ha visto hasta ahora, un tema recurrente en el examen de los daños derivados de la inclusión indebida de datos de solvencia en un fichero de morosos es el de la afectación del derecho al honor del interesado. Ahora bien, no siempre que se vulnera la norma de protección de datos se presenta al mismo tiempo una intromisión ilegítima al honor. Una buena muestra de ello puede encontrarse en el caso ya referido de la Audiencia Provincial de Segovia de 25.4.2002. Existía entre las partes una deuda cierta, vencida y exigible, que se incluyó en el fichero de morosos. No obstante, no hubo requerimiento de pago previo. La cesión de datos no implicaba una falsa morosidad ni mucho menos una lesión a la dignidad de quien realmente había incumplido su obligación de pagar. Sin embargo, la falta del requerimiento previo dio lugar a una vulneración de uno de los requisitos establecidos por la LOPD, conforme se ha visto más arriba.

En el mismo sentido, es posible incluir en los ficheros información errónea, que por no corresponder a la realidad infringe la LOPD, sin constituirse en vulneración al honor por no tener connotación peyorativa alguna, como en el caso de indicar que el afectado es avalista o fiador de una deuda (véase en este sentido la STS [1ª] de 29.1.2014 [Roj STS 434/2014]). En todo caso, lo que siempre debe haber es una vulneración de la LOPD que cause un daño «en los bienes o derechos» de la víctima (art. 19 LOPD). Es decir, puede en abstracto haber o no afectación del honor, pero para que haya responsabilidad conforme a esta Ley tiene que haberse vulnerado el régimen relativo al tratamiento de datos personales.

Seguramente podrían imaginarse más hipotesis en las cuales exista un tratamiento indebido de datos personales sin que necesariamente concurra una vulneración a derechos de la personalidad distintos del derecho de la protección de datos (como el caso del avalista ya citado). Sin embargo, ni a nivel jurisprudencial ni doctrinal existe una posición clara sobre cómo debe ser el régimen de responsabilidad a aplicar.

Como alternativa a lo anterior, podría adoptarse una posición reduccionista, conforme a la cual el derecho a la indemnización por vulnerar la LOPD procedería solo y en tanto se vulnerasen los derechos de la personalidad protegidos por la LO 1/1982 (especialmente el honor, según se ha visto). La mera existencia de una vulneración de los requisitos establecidos por la LOPD podría servir de base para presumir que se ha producido un daño en el sentido de la LO 1/1982.[23] En consecuencia, una interpretación

23 En esta línea, Grimalt Servera, P. (1999). La responsabilidad civil en el tratamiento automatizado de datos personales. Granada, Comares, 140.

sistemática de la ya examinada LO 1/1982 (art. 9) y la LOPD podría dar pie para entender que siempre que haya un tratamiento ilegítimo de datos en los términos previstos por la LOPD y normativa que la desarrolla se podrá presumir un daño en ese sentido. Con todo, conviene advertir que la LOPD no ha previsto, al menos de forma expresa, una presunción de este tipo.[24] En esta materia, como sucede en tantos otros casos, debe aplicarse la regla general de que quien alegue un daño deberá probarlo.[25]

Como en parte ya se ha apuntado, la LOPD establece una norma muy parca o sucinta que, por ejemplo, no aclara si la responsabilidad es por culpa o independiente de ella (es decir, objetiva). Tampoco los tribunales han acabado de definir las características del derecho a indemnización previsto por la LOPD.[26] Por ejemplo, nada se prevé sobre el doble nivel de análisis de la causalidad y la imputación objetiva, por lo que resultarían aplicables las reglas generales.[27]

La falta de un desarrollo legal más completo del régimen de responsabilidad por la vulneración de la LOPD ha propiciado estrategias de defensa escudadas en la ausencia de una actuación propia, como sucede con la alegación del titular del fichero de que el responsable no es él, sino quien proporcionó los datos erróneos. De ese modo se pretende escapar a la acusación de haber actuado negligentemente, como si al titular del fichero no le correspondiese también un deber de comprobar que desarrolla su servicio de información de una forma veraz, en la línea exigida por la Ley.[28] Justamente, es la ya referida función del fichero como «medio de presión» la que obliga a que su titular extreme la diligencia para que se cumplan los requisitos legales y no se causen daños a terceros.[29]

En fin, la inclusión incorrecta o indebida de datos personales en ficheros de morosos ha comenzado a nutrir un grupo de sentencias judiciales que se pronuncian sobre la responsabilidad civil, en general en conexión con la lesión del honor. Es previsible que lo hagan repetidamente en el futuro, dadas las incertidumbres que a día de hoy plantea el

24 Véase Aberasturi, cit., 184.

25 En la línea defendida por Parra, cit., 100.

26 Parecidamente, puede verse Aberasturi Gorriño, U. (2013). El derecho a la indemnización en el artículo 19 de la Ley Orgánica de protección de datos de carácter personal. *Revista Aragonesa de Administración Pública* (41-42), 173-206, 177.

27 En esta línea puede verse Lagunas Reyes, L. (2014). *La responsabilidad civil derivada de la inclusión indebida en un registro de morosos.* Trabajo Final de Máster. Pamplona, Universidad Pública de Navarra, <http://academica-e.unavarra.es/bitstream/handle/2454/9628/Lucia%20Lagunas.pdf?sequence=1> (consultado: 10.3.2014), 57.

28 En este sentido, véase Parra, cit., 111, y Rubio, cit., 95, con más referencias.

29 Véase Mendoza Losana, A. (2013). Registros de morosos, deudas dudosas y derecho al honor. *Cuadernos Civitas de Jurisprudencia Civil* (93), 487-515, 500.

marco legal vigente. En este sentido, una mayor precisión sobre los deberes que afectan a las partes en este tipo de situaciones, así como sobre la relación entre la protección de datos personales y otros intereses o bienes jurídicos protegidos, podría contribuir a clarificar el panorama de la responsabilidad civil en este ámbito.

6. BIBLIOGRAFÍA

Aberasturi Gorriño, U. (2013). El derecho a la indemnización en el artículo 19 de la Ley Orgánica de protección de datos de carácter personal. *Revista Aragonesa de Administración Pública* (41-42), 173-206.

Cuena Casas, M. (2014). Préstamo responsable, información crediticia y protección de datos personales. Revista de derecho concursal y paraconcursal (20), 161-185, también disponible en <http://www.elnotario.es/images/pdf/PRESTAMO_RESPONSABLE.pdf> (consultado: 10.3.2014).

Grimalt Servera, P. (1999). La responsabilidad civil en el tratamiento automatizado de datos personales. Granada, Comares.

Hualde Manso, T. (2013). Ficheros de morosos, nulidad del Reglamento de Protección de Datos y Derecho al Honor. *Revista Doctrinal Aranzadi Civil-Mercantil* (8), 49 - 58.

Lagunas Reyes, L. (2014). *La responsabilidad civil derivada de la inclusión indebida en un registro de morosos.* Trabajo Final de Máster. Pamplona, Universidad Pública de Navarra, <http://academica-e.unavarra.es/bitstream/handle/2454/9628/Lucia%20Lagunas.pdf?sequence=1> (consultado: 10.3.2014).

Linares Gutiérrez, A. (2011). La inclusión de datos en ficheros sobre solvencia patrimonial: cuestiones controvertidas. Crítica a la Sentencia del Tribunal Supremo de 15 de julio de 2010. *Dereito* (21), 217.232 <http://www.usc.es/revistas/index.php/dereito/article/view/830/805> (consultado: 10.3.2014)

Mendoza Losana, A. (2012). Guía práctica sobre la inclusión en un registro de morosos. *Revista CESCO de Derecho de Consumo* (4), 142 – 159.

Mendoza Losana, A. (2013). Registros de morosos, deudas dudosas y derecho al honor. *Cuadernos Civitas de Jurisprudencia Civil* (93), 487-515.

Parra Lucán, M. Á. (2011). Registro de morosos: Derecho civil y nulidad (parcial) del reglamento de desarrollo de la Ley Orgánica de protección de datos. *Revista Aranzadi Civil Doctrinal* (3), 81 – 113.

Parra Lucán, M.Á. / Lalana del Castillo, C. (2011). *La protección de los consumidores ante las empresas de telefonía, gas y electricidad. estudio de cuestiones jurídicas.* Zaragoza, Ayuntamiento, <https://www.zaragoza.es/contenidos/consumo/omic_proteccion_consumidores.pdf> (consultado: 10.3.2014)

Pérez de Ontiveros, C. (2012). Ficheros de solvencia patrimonial y de crédito: Cuestiones civiles y su apreciación por los tribunales del orden Contencioso-Administrativo. *Revista Aranzadi de Derecho Patrimonial* (28), 147- 183.

Plaza Penadés, J. (2013), Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en Internet, en: Plaza Penadés, J. (dir.), *Derecho y nuevas tecnologías de la información y la comunicación,* Cizur menor: Thomson Reuters Aranzadi, 1133-1174.

Rubio Torrano, E. (2012). Inclusión indebida en fichero de morosos. Intromisión ilegítima en el derecho al honor. *Revista Aranzadi Civil-Mercantil* (7), 91-95.

FACULTAD DE CONTROL EMPRESARIAL Y EL DERECHO A LA LIBERTAD INFORMÁTICA DE LOS TRABAJADORES: UN DERECHO FUNDAMENTAL (INEXPLICABLEMENTE) OLVIDADO

Ignasi Beltran de Heredia Ruiz
Profesor Agregado y TU acreditado de Derecho del Trabajo y de la Seguridad Social
Universitat Oberta de Catalunya (UOC)

RESUMEN: El estudio analiza el conflicto que suscita la capacidad de control del empresario sobre la actividad de los trabajadores y, particularmente, sobre el uso de los medios electrónicos propiedad de la empresa y su derecho a la libertad informática. Ante la ausencia de normas laborales que explícitamente den respuesta a este conflicto, el ensayo que se propone pretende exponer los criterios hermenéuticos empleados por los órganos jurisdiccionales laborales para resolver estas situaciones. En este sentido, la jurisprudencia ha establecido una amplia capacidad de control por parte del empresario. De modo que únicamente la existencia de una expectativa fundada y razonable de confidencialidad por parte del trabajador puede deslegitimar el posible examen de los medios informáticos de titularidad empresarial puestos a su alcance.

El ensayo defiende que, en ocasiones, la recopilación de datos efectuada por el empresario para poder evidenciar conductas inadecuadas de los trabajadores se ha desarrollado vulnerando el derecho a la libertad informática. Convirtiéndose en una dimensión constitucional del conflicto que inexplicablemente es omitida por los Tribunales y, en el mejor de los casos, queda en un plano secundario.

PALABRAS CLAVE: Poder de dirección y control empresarial, derecho a la libertad informática, privacidad, intimidad, medios informáticos propiedad empresa, internet.

1. CONTRATO DE TRABAJO, CONTROL EMPRESARIAL Y LIBERTAD INFORMÁTICA: UN ESPACIO CON UN ALTO POTENCIAL INTRUSIVO (PLANTEAMIENTO)

En una relación laboral son múltiples les datos que el trabajador debe suministrar al empresario. Más allá de los supuestos de transmisión expresa y consentida de datos de carácter personal o los que el empresario pueda exigir para la perfección del contrato y el desarrollo ordinario de la relación laboral, el uso intensivo de dispositivos electrónicos/digitales describe en este ámbito un escenario particularmente amenazador. Y esto es así, especialmente porque, como es bien sabido, permite (sin excesiva dificultad) el rastreo de un conjunto heterogéneo de datos que, pese a tener un carácter intrascendente (o poco relevante) si se analizan aisladamente, en cambio, si se almacenan, combinan y se

someten globalmente a un tratamiento mecanizado, pueden permitir una reconstrucción profunda y detallada del perfil individual del trabajador.

Este escenario resulta particularmente intrusivo, especialmente, porque el empleado, a través del uso de estos dispositivos en el quehacer ordinario de su labor profesional, inconscientemente, puede estar contribuyendo a configurar un perfil detallado de su personalidad y/o su conducta (o una particular dimensión de ambas)[1].

Siguiendo el criterio de la STSJ Cantabria 18 de enero 2007[2], «existen ciertas diferencias entre las nuevas tecnologías y los (…) medios audiovisuales y de comunicación; así, a diferencia de la video-vigilancia, en la ciber-vigilancia es posible distinguir dos momentos distintos, un primer momento de recogida de datos y un segundo momento de tratamiento de los datos obtenidos; es decir, aunque la informática permite un control directo del comportamiento laboral del trabajador, el verdadero conocimiento sobre el comportamiento del trabajador no se obtiene sino mediante la recogida sistemática de datos, su almacenamiento y su posterior tratamiento; de ahí que los limites que se derivan del respeto al derecho de la intimidad han de operar en dos momentos distintos: en el momento de la recogida de los datos y de la información, que ha de ser adecuados al fin perseguido, que no podrá ser otro que la verificación del cumplimiento de sus obligaciones laborales por el trabajador, y, además, en el momento del posterior registro físico para el tratamiento de los datos capturados».

---

1 El TC ha afirmado que «el que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta» (STC 143/1994).
En paralelo, la STC 292/2000 declara que «el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

2 AS 2007\1030.

En definitiva, su «privacidad»[3] (o una dimensión de la misma) puede llegar a ser (totalmente) transparente para el empresario.

La llamada 'libertad informática' (o «autodeterminación informativa»), precisamente, confiere el derecho a controlar el uso de los mismos datos insertos en un programa informático –habeas data– y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (STC 254/1993).

Llegados a este estadio, la distinción entre el derecho a la intimidad y el derecho a la libertad informática es relevante, por cuanto que mientras que el primero se protege desde la propia abstención de los sujetos que eventualmente pueden lesionar el derecho; la tutela informática requiere, además, la adecuación de su comportamiento con una acción concreta: suprimir datos, modificarlos, restringir su uso, emplearlos para fines legítimos, etc. (Arias Domínguez y Rubio Sánchez, 2006, versión digital)[4].

Sin embargo, esta es una circunstancia que ha sido analizada profusamente por la doctrina laboral y, sin duda, su exposición excede, con mucho, el espacio reservado para un ensayo de estas características. Apartándonos de este propósito, el objeto de este breve trabajo consiste precisamente en analizar (brevemente) el tratamiento que los Tribunales laborales están dispensando a esta dimensión de los derechos fundamentales. Especialmente, porque, adelantando las conclusiones, no parece que esté recibiendo el tratamiento aplicativo e interpretativo adecuado por parte de los órganos jurisdiccionales laborales. Veamos, a continuación, estos extremos.

---

3 Según la Exposición de Motivos de la LO 5/1992, 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, afirma que «la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado».

4 Como afirma la STSJ País Vasco 17 de abril 2012 (AS 1676): «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre datos personales que faculta a la persona para decidir cuales de esos datos proporciona a un tercero o cuales puede este tercero recabar y también permiten al individuo saber quien posee esos datos y para que se poseen pudiéndose oponerse a lo mismo. Por ello esos poderes de disposición y control que constituyen parte del contenido del Derecho Fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida obtención de acceso a los datos personales y su posterior almacenamiento y tratamiento así como su uso o posibles usos por terceros. Los complementos indispensables son, por un lado, la facultad de saber en todo momento quien dispone de esos datos y por otro a que uso los está sometiendo, para poder oponerse a esa posesión y usos».

2. CONTROL EMPRESARIAL, INTIMIDAD Y LIBERTAD INFORMÁTICA EN EL ÁMBITO LABORAL: OMISIONES RELEVANTES

La jurisdicción laboral ha prestado especial atención al uso extralaboral de los medios TIC propiedad de la empresa por parte del trabajador durante el tiempo de trabajo. Especialmente, desde el prisma de la capacidad de control que ostenta el empresario, de la transgresión o no de la buena fe contractual por parte del trabajador y de su derecho a la intimidad y al secreto de las comunicaciones. Como es bien sabido, la ausencia de disposiciones normativas específicas al respecto, ha llevado a la doctrina constitucional[5] y a la jurisprudencia a establecer algunos criterios hermenéuticos (la ausencia de una regulación interna o convencional regulando el uso extralaboral de estos dispositivos comunicada fehacientemente, crea una expectativa de confidencialidad en esos usos), hoy en día, consolidados por los propios Tribunales y la comunidad científica[6].

En este sentido, sorprende que el Legislador Laboral en alguno de los «arrebatos» reformadores que ha tenido en los últimos años no haya tomado la decisión de «normativizar» estos criterios a fin de dar una mayor seguridad a los operadores jurídicos (y aliviar a los órganos jurisdiccionales de una labor que en absoluto les corresponde). De hecho, como botón de muestra, el principal instrumento normativo para dar respuesta a estas cuestiones, el art. 18 ET, sigue refiriéndose al control de las «taquillas» del trabajador.

En paralelo, como recoge la STSJ Cantabria 18 de enero 2007[7], «después de establecer en el art. 20.3 que «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso», no hace ninguna referencia a esta novedosa forma de vigilancia, lo cual es tanto como decir que el ET no prohíbe el control empresarial mediante al utilización de las nuevas tecnologías de la información; en este sentido la

5 STC 170/2013. Pronunciamiento, en virtud del cual, siguiendo la síntesis de Monereo Pérez y López Insua (2014, versión digital) sostiene – adoptando un criterio muy restrictivo del derecho a la intimidad de los trabajadores - que «la mera «sospecha» acerca de si un trabajador transmite o no indebidamente información confidencial de su empresa a otra entidad mercantil, constituirá causa suficiente para que el empresario esté legitimado para comprobar tanto el contenido de los mensajes «SMS» del móvil profesional del trabajador, como del disco duro del portátil proporcionado por su empresa».

6 SSTS 26 de septiembre 2007 (RJ 7514); y 8 de marzo 2011 (RJ 932); 6 octubre 2011 (RJ 7699); y en la doctrina judicial, entre otras, SSTSJ Castilla-La Mancha 14 de abril 2011 (núm. 450/2011); y Galicia 25 de enero 2011 (núm. 503/2011). Y en la doctrina, **vid. al respecto, en**tre otros, Beltran de Heredia Ruiz (2010), p. 617 y ss.; y Calvo Gallego (2012), versión digital.

7 AS 2007/1030.

Agencia de Protección de Datos tiene establecido que "... en principio y de modo general, siempre que el correo electrónico, archivo informático etc. o cualquier otra comunicación formen parte de la actividad laboral del trabajador y se realicen en tiempo de trabajo puede ser analizadas y supervisadas por el empresario dado que entrarían dentro de la potestad de control que puede ejercer legalmente"».

El foco de atención en estos casos acostumbra a girar en torno a la intensidad con la que debe protegerse la intimidad de los trabajadores o, dicho de otro modo, en qué circunstancias prevalece la capacidad de control por parte del empresario. Sin embargo, éste no es el único derecho fundamental que puede verse vulnerado, pues, si se prevé un control de estos instrumentos informáticos es probable que también se esté procediendo a una recogida sistemática y exhaustiva de datos memorizados sobre aspectos del comportamiento del trabajador. Y, por consiguiente, el derecho a la libertad informática puede verse afectado.

De todos modos, como es bien sabido, no existe una norma que atienda específicamente a las particularidades que presenta la relación laboral, debiéndonos remitir a la Ley Orgánica 15/1999, de Protección de Datos (en adelante, LOPD). Los elementos conceptuales sobre los que se sustenta esta normativa son el principio de congruencia y racionalidad[8], por un lado; y el principio de consentimiento o autodeterminación[9], por otro.

---

8 En primer lugar, que no se proceda a una recolección de datos excesivos, en relación con el ámbito y las finalidades para las que se hayan obtenido (principio de pertinencia); exigiéndose la veracidad y actualización de los mismos (principio de veracidad) – vid. al respecto STC 94/1998. Además, el art. 4.2 LOPD, dispone que «los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos» (principio de finalidad); prohibiéndose en el art. 4.7 LOPD «la recogida de datos por medios fraudulentos, desleales o ilícitos» (principio de legalidad). Por otra parte, debe garantizarse la accesibilidad a los mismos, así como su posible cancelación, sin que puedan ser conservados durante un tiempo superior al necesario para los fines que justificaron su recogida (principios de accesibilidad, cancelación y descontextualización). Sin olvidar los denominados «datos sensibles», que según su tipología exigen un consentimiento expreso y por escrito (art. 7.2 LOPD), o bien, un consentimiento expreso (7.3 LOPD) –sin olvidar las excepciones previstas en el art. 7.6 LOPD. En todo caso, debe tenerse en cuenta que el empresario en todo caso debe abstenerse de indagar, almacenar, procesar o retener informaciones de tal naturaleza.

9 Esto es, el consentimiento consciente e informado (principio de autodeterminación), salvo que la Ley disponga otra cosa (art. 6.1 LOPD) –como se prevé para el ámbito laboral en el art. 6.2 LOPD– datos estrictamente necesarios para el desarrollo de la relación laboral; y los arts. 22 LPRL y 12.4 TRLISOS –para datos relativos a la salud. Para el resto de datos que no tengan esta naturaleza o los particularmente protegidos (ideología, salud, origen racial, etc.) deberá exigirse el consentimiento del trabajador. Y para el caso de que el responsable del fichero pretenda ceder determinados datos legalmente obtenidos a un tercero, también deberá recabar el consenti-

La incardinación del primero de estos principios en el ámbito laboral implica que el empresario, en el ejercicio de sus facultades, está habilitado legalmente para recabar información de diversa naturaleza de sus trabajadores, siempre que la emplee para las finalidades específicamente descritas en la normativa laboral, sin que en ningún caso, pueda destinarla a otros usos, pues, de otro modo, estaría incurriendo en una práctica ilícita[10].

Y, en relación al segundo de los principios, es importante reparar que a pesar de que el empresario, según los casos, pueda estar eximido de requerir el consentimiento del trabajador, esto no obsta a que éste tenga derecho a saber sobre su existencia y el tratamiento que se está llevando a cabo. De modo que, siempre que los datos hayan sido obtenidos de un modo lícito, una vez creado el fichero, el sistema de garantías debe prevalecer. Esto es, el responsable del mismo o su representante, dentro de los tres meses siguientes al momento del registro de los datos (salvo que ya hubiera sido informado con anterioridad), deberá informar al trabajador previamente de modo expreso, preciso e inequívoco sobre el contenido del tratamiento y la procedencia de los datos y de los siguientes extremos (art. 5.4 LOPD):

- de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información;
- de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
- y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

De modo que si el trabajador no ha sido informado sobre las circunstancias particulares que justifican la existencia de un fichero, así como del alcance y ámbito de aplicación del mismo debe calificarse como ilegal.

Sin olvidar, finalmente, que los datos registrados no pueden permanecer en posesión del responsable del fichero de un modo indefinido, sino que una vez cese la finalidad para la cual los datos fueron recogidos y registrados deben suprimirse (art. 4.5 LOPD).

Y esta matriz (brevemente expuesta) describe, precisamente, la clave de bóveda del conflicto entre el derecho a la libertad informática y el poder de control por parte del empresario, pues, la digitalización de gran parte de los dispositivos a disposición de los trabajadores y de sus comunicaciones y, en particular, la extraordinaria facilidad para su eventual almacenamiento coloca al empresario ante la necesidad de dar cumplimiento

---

miento del trabajador afectado (art. 11.1 LOPD), salvo que concurra algunas de las excepciones previstas en el art. 11.2 LOPD.

10 La jurisprudencia constitucional ha tenido ocasión de pronunciarse en dos supuestos al respecto: SSTC 11/1998; y 202/1999.

de los deberes descritos en la LOPD. En caso contrario, debería considerarse que se ha vulnerado los derechos fundamentales de los trabajadores.

Por ejemplo, a pesar del contenido del art. 20.3 ET, debe entenderse que el tratamiento de datos emitidos por el sistema de GPS instalados en los vehículos debe cumplir con lo dispuesto en la LOPD. Esto es, debe informarse al trabajador según lo previsto en el art. 5.1 LOPD[11].

Lo «curioso» (y/o –a nuestro entender– sorprendente) del caso es que, si bien es (relativamente) frecuente que el derecho a la intimidad del trabajador en el uso extralaboral de estos dispositivos ceda frente a la capacidad de control del empresario y, por consiguiente, los Tribunales –en base a los datos obtenidos– admiten la resolución del contrato por vulneración de la buena fe contractual, la dimensión de la libertad informática no aparece ni siquiera mencionada. O, mejor dicho, lo hace en contadas ocasiones[12].

Y, dentro de éstas, resulta particularmente ilustrativa la STSJ Cantabria 18 de enero 2007[13]. Como se sostiene en la misma, es cierto que aunque «no se halle vedada la utilización de las nuevas tecnologías entre los instrumentos disponibles para el control y vigilancia de la actividad laboral, no comporta que su aplicación pueda hacerse de manera omnímoda e indiscriminada, con abstracción de los derechos fundamentales del trabajador, tal como se subraya, en sus diversos considerandos, por la Directiva 1995/46CE». Y, más concretamente, es exigible que se respete el «derecho a una vida privada, en cuya virtud el trabajador debe gozar de una razonable expectativa a un cierto grado de intimidad, dignidad, confidencialidad y autonomía»[14].

A partir de estos parámetros, en este pronunciamiento se declara que, a pesar de que la empresa notificó con carácter previo a los trabajadores la prohibición del uso del ordenador para fines extralaborales, se produjo una vulneración de su derecho a la libertad informática porque se instaló un software para su monitorización que excedía de la finalidad perseguida. En concreto, en la medida que «la recogida de datos no se limitaba a

11 Informe AEPD 2008\193.

12 Como botón de muestra (y con el rigor relativo que se le pueda atribuir a un «experimento» de este tipo), en una búsqueda jurisprudencial en el orden Social en la base de datos «Westlaw-Aranzadi», son muy pocos los resultados que aparecen a los términos «libertad informática» (15); «autodeterminación informativa» (9); «habeas data (4).

13 AS 2007\1030.

14 En la STJS Comunidad Valenciana 16 de febrero 2010 (AS 945) se estima que se ha producido una violación del derecho a la autodeterminación informativa (y a la intimidad), pues, la empresa sin haber establecido previamente un protocolo sobre el uso de los medios informáticos en el tiempo de trabajo, procede unilateralmente a auditar la seguridad del sistema informático, averiguando la utilización de todos los empleados de sus visitas a internet; describiendo no solo su número de visitas sino también las concretas páginas visitadas. En términos similares, STSJ País Vasco 17 de abril 2012 (AS 1676).

realizar una estadística de los accesos a Internet que no fueran los oficiales de la pagina de la [empresa] y los enlaces permitidos por esta, sino que especificaba asimismo los recursos de Internet solicitados (paginas web, gráficos, fotografías...etc.), y tal acopio de datos, en la medida en que entrañaba un control sistemático de los sitios visitados, así como de su frecuencia, tiempo de conexión y navegación, permiten reconstruir aspectos subjetivos relativos a la intimidad del trabajador, y ello excede sin duda de la finalidad declarada: conocer el uso que se hacía de Internet en horas de trabajo, que era el parámetro que debió modular el nivel y la intensidad de la recogida de datos, y que al ser rebasado deslegitima el comportamiento empresarial, pues constituye un principio básico de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que sólo se podrán recoger datos de carácter personal para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido (art. 4.1), lo que también se deduce del Considerando 28 de la Directiva 1995/46 cuando indica que «todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos».

En cambio, en la STSJ Comunidad Valenciana 28 septiembre de 2010[15] se alcanza una solución dispar. Se trata de un supuesto en el que una empresa, tras entregar a todos los trabajadores una carta (que firman) en la que se les comunica que queda terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, internet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo, procede a la monitorización de dos trabajadores porque tiene sospechas de que están incumpliendo este protocolo. En concreto, realiza un control de sus ordenadores a través de un software que permite realizar capturas de pantalla. En opinión del Tribunal, obviando (por completo) la dimensión relativa al derecho a la libertad informática, se trata de un sistema de control «pasivo o poco agresivo», pues, se «limita» a capturar lo que está en pantalla, para comprobar el uso del ordenador por parte del trabajador. De modo que la medida adoptada necesaria, idónea, justificada y equilibrada. Además, –añade– este sistema no supone una invasión de su intimidad, «toda vez que la contraseña utilizada (…) impedía el acceso a sus archivos y el sofware instalado, como se dijo, sólo permitía la recuperación de pantallas.

Pese a esta disparidad de criterios entre esta doctrina judicial expuesta, posteriormente, la STS 6 de octubre 2011[16] entendió que no se daba la contradicción necesaria para poder entrar en el fondo. No obstante, esta sentencia de TS es muy ilustrativa de la línea interpretativa imperante en la jurisdicción social, pues, se afirma que «En el caso

15 AS 2011\47.

16 RJ 7699.

del uso personal de los medios informáticos de la empresa no puede existir un conflicto de derechos cuando hay una prohibición válida». De modo que «si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo».

Así pues, «sentada la validez de prohibición tan terminante, que lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no es posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición. Tal entendimiento equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario de acuerdo con lo dispuesto en el art. 20 ET».

Criterios hermenéuticos que quedan consolidados con la STC 170/2013 al afirmar que «La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe».

Sin embargo, a nuestro entender, esta matriz interpretativa expuesta resulta muy preocupante, especialmente, porque con independencia del sentido final de los fallos, los Tribunales están omitiendo el posible impacto de las medidas de monitorización empresarial sobre el derecho a la autodeterminación informativa (y su eventual o no vulneración). Sin obviar que, como afirma el Voto Particular de la STSJ Castilla y León\Valladolid 5 de diciembre 2012[17] esta capacidad de control empresarial admitida por la STS 6 de octubre 2011, «no excluye la posible vulneración del derecho a la intimidad cuando el seguimiento empresarial alcance a determinados aspectos íntimos del trabajador, como pudieran ser conversaciones privadas a través de chats, correos electrónicos y otras aplicaciones, esto es, cuando el seguimiento exceda del criterio genérico de proporcionalidad, con sus tres elementos constitutivos (necesidad, idoneidad y proporcionalidad)». O, siguiendo con el citado voto particular, «El Tribunal Supremo no ha declarado la procedencia de todos los despidos basados en un uso personal del ordenador y de las redes informáticas empresariales, ni creo que haya concedido una habilitación genérica a la dirección de las empresas para llevar a cabo un seguimiento exhaustivo de la actividad de sus empleados en la red. Es más, ni siquiera podía hacerlo en los estrechos márgenes del recurso de casación para la unificación de doctrina. Entenderlo así es una magnificación inasumible».

17 AS 2013\167.

Sin olvidar que «una cosa es que en determinadas circunstancias el empresario quede eximido de requerir el consentimiento del trabajador, y otra muy distinta es que el éste desconozca la existencia de un fichero de datos y el tratamiento que se está haciendo de los mismos»[18]. No obstante, por el momento, esta opinión (lamentablemente) tiene una predicación minoritaria. Ahondando en este enfoque de la jurisprudencia descrita por la STS 6 de octubre 2011[19], la STSJ Andalucía\Granada 13 de noviembre 2013[20] declara que la existencia de una prohibición absoluta y legítima de uso personal de estos medios de la empresa en horario de trabajo, excluye la necesidad por parte de la empresa de informar a los trabajadores de la existencia de un software que permita la monitorización de su uso (a través de un programa que capta un fotograma cada diez segundos y posteriormente es archivado durante un período de seis meses).

Repárese que en este caso, el software instalado permite un control indiscriminado de todos los trabajadores, con independencia de que haya sospecha o no de la existencia de un uso incorrecto o de un incumplimiento del protocolo de la empresa firmado por los trabajadores. Pero, a mayor abundamiento, aunque haya una prohibición de uso extralaboral de tales medios, la potencial violación del derecho a la libertad informática no queda excluida per se. O, dicho de otro modo, la recopilación sistematizada y mecánica de la actividad estrictamente laboral del trabajador (y ajustada al protocolo fijado por la empresa y consentido por empleado) puede ser reveladora de ciertos aspectos de su vida personal que son susceptibles de amparo constitucional. Dimensión, de nuevo, soslayada por los órganos jurisdiccionales.

Otro ejemplo (a nuestro entender) preocupante: la STSJ Castilla y León\Valladolid 5 de diciembre 2012[21] declara la procedencia del despido de una trabajadora porque lleva a cabo un uso particular de Internet que supera la media de estadística efectuada por la empresa y más de un 70% de las páginas a las que accede durante su jornada laboral corresponden a categorías ajenas a su actividad laboral en contra de la prohibición expresa de la empresa (pero sin que quede verificada la incidencia de tal dedicación extralaboral en el tiempo de trabajo, rendimiento o productividad). En concreto, la empresa a través de su Código de Conducta Telemática establece que «todas las páginas de Internet a las que accedan los trabajadores de IMESAPI, S.A. son registradas y almacenadas por el período legal establecido (dos años). La información almacenada incluye entre otras informaciones: usuario, equipo, fecha, hora, página visitada...».

Sin embargo, como recoge el Voto Particular de este pronunciamiento, debe tenerse en cuenta que conforme a la STJUE 19 de abril 2012 («Bonnier Audio AB y

18 Sagardoy Bengoechea (2005), p. 78.

19 RJ 7699.

20 AS 2013\2935.

21 AS 2013\167.

otros contra Perfect Communication Sweden AB», asunto C-461/10), «la identificación de la persona que se conecta a una red a partir de la dirección IP del correspondiente dispositivo de transmisión de datos (que es lo que consta en hechos probados que se ha hecho en este caso) supone comunicar y tratar datos personales y los Estados miembros deben procurar basarse en una interpretación de las Directivas comunitarias que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico de la Unión y muy especialmente el principio de proporcionalidad, que es interpretado en términos idénticos a los contenidos en la jurisprudencia constitucional española (necesidad, idoneidad y proporcionalidad en sentido estricto) para garantizar un justo equilibrio entre los bienes jurídicos implicados».

3. VALORACIÓN FINAL

Los Tribunales están admitiendo un amplio control por parte del empresario de los instrumentos electrónicos propiedad de la empresa puestos a disposición de los trabajadores, siempre que haya directrices (conocidas por los trabajadores) que fijen las condiciones para su uso extralaboral. En este escenario, la intimidad del trabajador queda en un plano secundario, pues de este modo, se entiende que ha quedado disipada toda expectativa razonable de confidencialidad e intimidad.

Sin pretender entrar en la idoneidad o no de esta línea interpretativa (pues, excede del objeto de este estudio), en el presente ensayo hemos tratado de evidenciar que el derecho a la «libertad informática» o «autodeterminación informativa» no debería verse afectado (o subyugado) por esta omnímoda facultad empresarial. Sino todo lo contrario, pues, dependiendo de las circunstancias puede permanece subyacente y de un modo autónomo/independiente en todas estas situaciones.

Lo que significa que, aunque existan estas directrices para el uso extralaboral de los medios electrónicos propiedad de la empresa, el empresario sigue estando obligado a dar cumplimiento a las directrices que marca la LOPD. En caso contrario, existe el riesgo (cierto) de que esté incurriendo en una conducta contraria a un derecho fundamental.

Sin embargo, esta dimensión del problema no está recibiendo, a nuestro entender, un tratamiento adecuado por parte de los tribunales e inexplicablemente es soslayada reiteradamente (salvo contadas ocasiones).

Esperamos que el contenido de este breve trabajo contribuya a sacarlo del ostracismo que padece.

4. BIBLIOGRAFIA

Beltran de Heredia Ruiz, I. (2010). Las tecnologías de la información y de la comunicación en el ámbito laboral. En Peguera Poch (coord.), Principios de Derecho de la Sociedad de la Información. Pamplona: Aranzadi – Thomson/Reuters.

Calvo Gallego, J. (2012). TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales. Revista Doctrinal Aranzadi Social, 9, versión digital (BIB 2012\56).

Monereo Pérez, J. L. y López Insua, B. M. (2014). El control empresarial del correo electrónico tras la STC 170/2013. Revista Doctrinal Aranzadi Social, 11, versión digital (BIB 2014\122).

Sagardoy Bengoechea, A. (2005). Los derechos fundamentales y el contrato de trabajo. Madrid: Thomson-Civitas.

INTERNET Y EL DERECHO A LA PROPIA IMAGEN: ALGUNAS NOTAS SOBRE SU PROBLEMÁTICA JURÍDICA[1]

Patricia Escribano Tortajada
Profesora de Derecho Civil de la Universitat Oberta de Catalunya y Universitat Jaume I de Castellón

RESUMEN: Internet en general y las redes sociales en particular, además de sus innumerables ventajas, se configuran como un marco idóneo para lesionar los derechos de sus usuarios. Básicamente, las vulneraciones más comunes se centran en el derecho a la protección de sus datos, pero también es muy fácil que se produzcan lesiones de los derechos de la personalidad, en concreto, el honor, la propia imagen y la intimidad. La Ley orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen ha tenido que dar respuesta tradicionalmente a las vulneraciones que se producían de estos derechos en los medios de comunicación «tradicionales», es decir, televisión, radio o prensa escrita. Sin embargo, la evolución de Internet y las redes sociales suponen un reto para esta norma, la cual deberá ir dando respuesta o amparo a los ataques que se produzcan de estos derechos. El objetivo de este trabajo es poner de relieve cuál es el estado de la cuestión o mejor dicho, cuáles son los nuevos problemas jurídicos que plantean la lesión de uno de esos derechos de la personalidad, en concreto, el de la propia imagen en el marco de Internet y las redes sociales y las dificultades existentes para dar una respuesta satisfactoria a dicha problemática.

PALABRAS CLAVE: Propia imagen, redes sociales, lesión, consentimiento.

1. INTRODUCCIÓN

En la actualidad, Internet es una herramienta esencial en todos los ámbitos de nuestra vida diaria. Lo utilizamos en el trabajo, en la universidad, en el colegio, para realizar compras, para ponernos en contacto con nuestros amigos y familiares o para compartir vídeos y fotos. Las utilidades que tiene son infinitas y la práctica mayoría de los usuarios no podrían plantearse ni concebir actualmente la vida sin el mismo. Sin embargo, a pesar de todas las ventajas que posee y las facilidades que nos proporciona, Internet se ha configurado como un marco idóneo para la posible vulneración y ataque de nuestros derechos, tanto de sus usuarios como de los ciudadanos en general. Algunos

1 Este trabajo está enmarcado dentro del proyecto de investigación financiado por el Ministerio de Economía y Competitividad «Derecho y redes digitales: hacia una redefinición jurídica del espacio público y privado» cuya referencia es DER2011-29637.

de los más proclives a sufrir lesiones son los derechos al honor, la intimidad y la propia imagen consagrados expresamente en el art. 18.1 de la Constitución Española. Este precepto fue desarrollado posteriormente por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante LO 1/1982)[2]. Sin embargo, ya adelantamos que el objeto de este trabajo no será el análisis de los tres, sino que nos vamos a centrar exclusivamente en la problemática que plantea Internet y el derecho a la propia imagen.

El uso de Internet, la proliferación de redes sociales y el aumento de sus usuarios desde edades muy tempranas hace que sea bastante sencillo lesionar estos derechos. Por otro lado, la LO 1/1982, norma básica en esta materia, es de hace más de treinta años y en ese momento el desarrollo de las nuevas tecnologías era incipiente, por no decir, prácticamente nulo. No olvidemos que el nacimiento de Internet se produce a finales de los años ochenta[3]. Aun así, hemos de tener en cuenta que la Constitución Española en 1978 ya tuvo en cuenta la posibilidad de que las nuevas tecnologías vulneraran nuestros derechos, al precisar el apartado cuarto del art. 18 que *«La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».* Por tanto, ¿es necesaria una reforma de la LO 1/1982? O ¿son los jueces los que tendrán que resolver caso por caso, intentando aplicarla a las lesiones del derecho a la propia imagen en Internet y en las redes sociales?

El objeto de estas líneas es analizar brevemente el concepto del derecho a la propia imagen y los nuevos problemas jurídicos con los que se puede encontrar, a la luz del cada vez más extendido uso de Internet y de las redes sociales. Nuestra intención es centrarnos en dos aspectos claves: la utilización de los fotomontajes y el tema del consentimiento para publicar fotografías en las redes sociales.

2. EL DERECHO A LA PROPIA IMAGEN

2.1. Cuestiones generales

Ya hemos dicho que el derecho a la propia imagen es uno de los derechos de la personalidad consagrados en nuestra Carta Magna, regulado en la LO 1/1982, de 5 de mayo. Aunque el objeto de estas líneas no sea analizarlo en profundidad, consideramos que, al menos, es necesario dejar apuntadas algunas cuestiones esenciales, para el mejor entendimiento de la problemática jurídica que suscita Internet y las redes sociales en relación con el derecho a la propia imagen. En primer lugar, hemos de destacar que,

2 BOE núm. 115 de 14 de mayo de 1982.

3 http://www.uv.es/~biblios/mei3/Web022.html#Project

aunque no es del todo una consideración uniforme, un gran sector de la doctrina y la jurisprudencia señalan que el derecho a la propia imagen, el derecho al honor y a la intimidad son tres derechos autónomos e independientes[4]. Lo que no es óbice, para que como consecuencia de la vulneración, en nuestro caso, del derecho a la propia imagen puedan producirse además, violaciones o ataques al honor o la intimidad.

En segundo lugar, por lo que respecta al concepto se ha definido por un lado «la imagen» y por otro, «el derecho a la propia imagen». En el primer caso, la STS de 30 de enero de 1998 la considera como «*la figura, representación, semejanza o apariencia de una cosa y a efectos de la Ley Orgánica 1/1982, equivale a representación gráfica de la figura humana, mediante un procedimiento mecánico –y con ello cualquier técnica adecuada– para obtener su reproducción*» (FJ único)[5]. En cuanto al derecho a la propia imagen, podemos traer a colación la STS de 24 de julio de 2012, que citando diversas sentencias del Tribunal Constitucional lo define en los siguientes términos: «*un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que pueden tener difusión pública y a impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad –informativa, comercial, científica, cultural, etc.– perseguida por quien la capta o difunde*» (FJ 6º)[6].

En tercer lugar, como ha señalado la sentencia que acabamos de citar y así también se desprende del art. 7 LO 1/1982, que hace referencia a las intromisiones ilegítimas, se habla de tres facetas diferentes: la obtención, la reproducción o publicación de la imagen.

---

4 A este respecto pueden citarse entre otras: la STS de 13 de julio de 2006 (RJ 2006\4969); SSTC de 22 de abril de 2002 (RTC 2002\83); de 2 de julio de 2001 (RTC 2001\156); de 26 de marzo de 2001 (RTC 2001\81). Puede verse un profundo análisis jurisprudencial de la materia en: Castilla Barea, M. (2011). *Las intromisiones legítimas en el Derecho a la Propia Imagen. Estudio de las circunstancias que legitiman la intromisión en la LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.* Navarra: Aranzadi, pp. 70 y ss. De Verda y Beamonte, J.R. (2011). El derecho a la propia imagen en la Ley orgánica 1/1982, de 5 de mayo. En José Ramón Verda Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.41- 65). Navarra: Thomson-Aranzadi, p. 62.

5 RJ 1998\358. Se pueden ver también entre otras las SSTS de 11 de abril de 1987 (RJ 1987\2703); de 21 de octubre de 1996 (RJ 1996\8577). No obstante, la STS de 30 de enero de 1998 (RJ 1998\358) señala que «*La interpretación no se agota en lo que se deja expuesto y en cuanto a que equivale a reproducción visible de figura humana identificada o identificable, pues cabe extender el concepto a otras representaciones de la persona que faciliten de modo evidente y no dubitativo o por aproximaciones o predisposiciones subjetivas, su recognoscibilidad*» (FJ 1º).

6 JUR 2012\311146.

Las conductas que se consideran como intromisiones ilegítimas respecto al derecho a la propia imagen son las del art. 7.5 y 7.6[7].

En cuarto lugar, hemos de poner de manifiesto la importancia del consentimiento, que es uno de los elementos clave para poder considerar una actuación como intromisión ilegítima. La norma habla de consentimiento «expreso», es decir, que en principio parece ser que no cabría un consentimiento tácito. Por lo que respecta a su significado se ha señalado que implica «*autorización, declaración por la que el titular del derecho a la imagen permite –consiente- la obtención, reproducción o la publicación de la propia*»[8]. Y que «*puede deducirse de actos o conductas de inequívoca significación, no ambiguas o dudosas*»[9]. Por otro lado, se considera también que el mismo puede ser anterior o posterior a la obtención, reproducción o publicación de la imagen[10]. Si lo ponemos en relación con las conductas señaladas en el art.7 LO 1/1982, se ha de precisar que el consentimiento dado por el titular para la captación de la fotografía no implica un consentimiento para la reproducción o publicación de la misma[11].

Por último, decir que para reputar como ilegítima una intromisión o no se tienen en cuenta también, otros criterios como el carácter público o privado del espacio donde se captó la fotografía, el ser un personaje público y el carácter accidental de la persona a la cual se le tomó la foto (art. 8 LO 1/1982).

2.2. Breve referencia a las caricaturas y los fotomontajes

El artículo 8.2.b) de la LO 1/1982 señala que no habrá intromisión ilegítima cuando se trate de la utilización de caricaturas de personajes públicos de acuerdo con el uso social. De ahí deriva que la ley está haciendo referencia a las personas de notoriedad

---

7 «*5. La captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2. 6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.*» O'Callaghan Muñoz, X. (1991). *Libertad de expresión y sus límites: honor, intimidad e imagen.* Madrid: EDERSA, p. 121 mencionando determinadas sentencias del TS considera que la enumeración de dicho precepto no es un *numerus clausus.* En el mismo sentido se pronuncia: Grimalt Servera, P. (2007). *La protección civil de los derechos al honor, a la intimidad y a la propia imagen.* Madrid: Iustel, pp. 63 y 64.

8 O'Callaghan Muñoz, X. (1991). *Libertad de expresión...*, *op.cit.* p. 137.

9 De Verda y Beamonte, E. y Soriano Martínez, E. (2011). El consentimiento como causa de exclusión de la ilegitimidad de la intromisión. En José Ramón Verda Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.67- 85). Navarra: Thomson-Aranzadi, p. 69 citando varias sentencias del Tribunal Supremo.

10 O'Callaghan Muñoz, X. (1991). *Libertad de expresión...*, *op.cit.* p. 137.

11 Castilla Barea, M. (2011). *Las intromisiones legítimas en el Derecho a la Propia imagen…, op.cit.,* pp. 149 y ss.

pública excluyendo a los ciudadanos «anónimos». Además, como ha señalado algún sector de la doctrina no cabría la caricatura de una persona privada[12]. No es objeto de este análisis realizar un estudio en profundidad sobre dichos conceptos, pero, consideramos que es necesario dejar apuntado al menos el concepto para entender uno de los problemas relacionados con el derecho a la propia imagen e Internet, ya que cada vez son más numerosos los fotomontajes que circulan en la red, sobre todo a raíz de algún acontecimiento de cierto impacto social[13] y que pueden afectar tanto a personajes públicos como aquellas que no lo son[14].

La caricatura ha sido definida como «*una representación gráfica, no necesariamente un dibujo o, en general, artística, en el que, de modo exagerado, se deforma la imagen de una persona, en clave humorística, y con carácter crítico, en el uso de la libertad reconocida en el art. 20.1 a) de la Constitución*»[15]. Mientras que no la habrá «cuando estemos antes una reproducción gráfica en la que la figura de la persona no aparezca deformada o la deformación no sea fácilmente reconocible»[16]. Pero ¿es lo mismo una caricatura que un fotomontaje? En principio no sería lo mismo. El TS en la sentencia de 7 de marzo de 2006[17] señaló en su FJ 4º que «*En cuanto al concepto de «caricatura», es cierto que su primera acepción en el Diccionario de la Lengua Española de la Real Academia, como «dibujo satírico en que se deforman las facciones y el aspecto de alguna persona», puede resultar un tanto estrecha, a los efectos de aplicación de la Ley Orgánica 1/82 de acuerdo con la realidad social, si por limitarla a los dibujos se excluyen las composiciones o montajes fotográficos, pues la acelerada expansión de la fotografía digital y de los programas informáticos de tratamiento de la imagen, hasta llegar a su actual divulgación al alcance del gran público, es un factor*

12 Blasco Gascó, F. de P (2008). Algunas cuestiones del derecho a la propia imagen. *Bienes de la personalidad. XIII Jornadas de la Asociación de Profesores de Derecho Civil.* Murcia: Editum. Ediciones de la Universidad de Murcia, p. 87.

13 Uno de los últimos hechos que más impacto ha tenido en las redes sociales ha sido el incidente que tuvo la presidenta del PP de Madrid cuando unos agentes de movilidad la estaban multando. Pueden verse algunos ejemplos de los fotomontajes en: http://www.huffingtonpost.es/2014/04/03/fotos-montajes-aguirre-fuga_n_5085388.html. Pero ha habido otros que también han tenido su impacto en las redes sociales como el del futbolista Ballotelli: http://listas.eleconomista.es/humor/1060-los-25-mejores-fotomontajes-de-balotelli.

14 El caso de la «Niña de las Burbujas».

15 De Verda y Beamonte, J.R. (2007). Las intromisiones legítimas en los derechos a la propia imagen y a la propia voz. Un estudio del art. 8.2 de la Ley Orgánica 1/1982, de 5 de mayo, a la luz de la reciente jurisprudencia. *Diario La Ley,* nº. 6754, Sección Doctrina, 11 de julio de 2007, Año XXVIII, p.10 de la versión electrónica.

16 De Verda y Beamonte, J.R. (2007). «1955 SENTENCIA DE 7 DE MARZO DE 2006: Intromisión ilegítima en el derecho a la propia imagen. *Cuadernos Civitas de jurisprudencia civil,* nº. 73, p. 335.

17 RJ 2006\1579.

determinante de que, en el ámbito jurídico, no sean en absoluto descartables las caricaturas mediante composiciones fotográficas (…) Aceptado, pues, que una caricatura puede consistir en un fotomontaje o composición fotográfica». Por lo que respecta al fotomontaje, la sentencia del Tribunal Constitucional de 27 de abril de 2010[18] consideró que: «*A estos efectos, resulta relevante tomar en consideración el hecho de que la publicación que constituye el objeto de nuestro juicio es un montaje irónico elaborado a partir de una fotografía de la actora civil superpuesta sobre un cuerpo ajeno. En la medida en que del contexto de la revista se desprende que la composición perseguía una finalidad humorística mediante la manipulación de la imagen, puede calificarse de caricatura, pues debe entenderse por tal toda creación satírica realizada a partir de las facciones y el aspecto de alguien, deformando su realidad. Con la generalización de las nuevas tecnologías de tratamiento de la imagen, esta categoría, que tradicionalmente se había basado exclusivamente en la dimensión humorística del dibujo, se plasma cada vez con más frecuencia en la alteración de fotografías originales, aunque no pierde por ello su esencia de creación irónica basada en la reelaboración de la fisionomía del modelo que tiene por objeto. En los casos en los que la caricatura se elabora mediante la distorsión de la imagen fotográfica de una persona, resulta evidente que se viene a afectar al derecho a la propia imagen de la persona representada, si bien tal afección puede venir justificada por el legítimo ejercicio de la libertad de expresión [art. 20.1 a) CE] o, incluso, de la libertad de creación artística [art. 20.1 b) CE].»* (FJ 5º).

La jurisprudencia menor ha tenido posibilidad de pronunciarse sobre algún supuesto de fotomontajes respecto a personajes no públicos. Es el caso de la sentencia de la Audiencia Provincial de las Islas Baleares de 10 de abril de 2008[19]. Por lo que respecta a los hechos, el demandante tuvo conocimiento, por parte de un compañero de trabajo, que en una gasolinera estaban vendiendo calendarios para el sorteo de una cesta de navidad. En los mismos había un fotomontaje en el que aparecía la cara manipulada de dicha persona sobre la figura de un perro. Según manifestó el demandante, el fotomontaje aparecía también en una página web caracterizada por su contenido humorístico. Demandó a la empresa gráfica que imprimió los calendarios, la cual alegaba que únicamente los había impreso, ya que la imagen la había sacado de Internet. El demandante solicita una indemnización de daños y perjuicios por la cantidad de 30.000 euros, debido al daño moral que se le había causado y que retirara la empresa gráfica todo el material que había difundido. Algunas cuestiones relevantes de la sentencia pueden sintetizarse en las siguientes: por un lado, el Fundamento de Derecho Segundo apunta que «*la captación y difusión de la imagen del sujeto sólo será admisible cuando la propia y previa conducta de aquél o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puede colisionar con aquél*».

18 RTC 2010\23.

19 AC 2008\1048.

Por otro lado, en el mismo fundamento se señala que estima la demanda porque considera que hay «*una intromisión ilegítima en el ámbito de protección delimitado por los artículos 1 y 2 de la referida Ley, y concretada en el supuesto del artículo 7.6, que define como tal «La utilización del nombre, de la voz o de la imagen de una persona fines publicitarios, comerciales o de naturaleza análoga», siendo especialmente reprochable dicha utilización en el caso de autos, a juicio del Tribunal, habida cuenta de que la imagen ha sido, además, distorsionada imitándola en una suerte de engendro entre hombre y perro, pero con suficiente referencia de los rasgos humanos como para identificar al individuo; apareciendo además en el calendario, al pie de la fotografía y para mayor mofa, la rúbrica que se dirá: «Clonan al primer hombre fiel»*». En último lugar, por lo que respecta al daño moral (aunque rebajó la cantidad solicitada) según la Audiencia se ha de tener en cuenta la difusión o audiencia del medio a través del cual se produce, «*siendo ese ámbito de la difusión intromisiva el que determina la mayor o menor entidad indemnizable por la entidad demandada*».

3. INTERNET Y LAS REDES SOCIALES: PROBLEMÁTICA JURÍDICA

3.1. Cuestiones generales

Como comentamos anteriormente, en la actualidad, los usuarios de Internet no pueden concebir la idea de vivir sin él. Prácticamente la casi totalidad, por no decir, la totalidad de los mismos tienen como mínimo una cuenta de correo electrónico, ven asiduamente vídeos en *Youtube,* pero como regla general, una parte importante forma parte de una red social. Algunas de las más utilizadas en la actualidad, o más extendidas, como todos sabemos son *Facebook*[20]*, Tuenti, Twitter, Google + o Linkedin*[21]. Estas redes sociales están en constante desarrollo, siempre con la finalidad de dar respuesta a los requerimientos o necesidades de sus usuarios o bien para «atraerlos» y que se den de alta en las mismas.

Lo que queremos poner de relieve es que el uso de las redes sociales está tan extendido que es bastante infrecuente, encontrar a alguien que no forme parte de una red social. Esto lo pone muy bien de manifiesto Dumortier cuando habla del «efecto de normalización de Facebook»[22]. Es más, el que una persona «no esté» en una red social

20 A lo largo de este trabajo cuando hablemos de redes sociales, utilizaremos como referencia Facebook, por ser en la actualidad una de las más utilizadas por los usuarios.

21 Para ver las distintas clasificaciones de redes sociales puede verse entre otros: Ortiz López, P. (2013). Redes sociales: funcionamiento y tratamiento de información persona. En Artemi Rallo Lombarte y Ricard Martínez Martínez (editores), *Derecho y Redes Sociales*. Navarra: Civitas y Thomson Reuters, pp. 23 y 24.

22 Dumortier, F. (2009). Facebook y los riesgos de la «descontextualización» de la información. *Revista de Internet, Derecho y Política,* número 9, p. 32, http://journals.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier

puede incluso conllevar a una especie de «automarginación social». Es decir, pongamos el caso de un grupo de varios amigos, la mayoría de los cuales «están» en Facebook excepto uno o dos. Esa mayoría de amigos estarán compartiendo determinadas fotos de actividades sociales que han realizado, vídeos, escribiendo comentarios en sus «muros», o quedando a través de los «eventos». Sin embargo, el amigo que no «esté» en Facebook no podrá participar de esas interacciones, lo que puede conllevarle a la sensación que está siendo apartado del grupo por no estar en la red social. Por decirlo de algún modo, las redes sociales «online» pueden estar desnaturalizando las propias «redes sociales off line»[23]. Obviamente, Internet y las redes sociales nos facilitan la vida, no podemos negarlo. Sin embargo, a pesar de sus múltiples ventajas se han configurado con un marco idóneo para la vulneración de derechos como la propia imagen[24]. Como se ha puesto de manifiesto, lo que caracteriza a las redes sociales, particularmente Facebook, respecto de los medios de comunicación tradicionales, es su facilidad, gratuidad e inmediatez, así como su alcance potencial[25]. De ahí la importancia de tener sumo cuidado a la hora de subir o compartir determinada información, en nuestro caso particular las fotos, ya que la difusión de las mismas puede tener un alcance considerable. Pero una cosa es que una persona suba sus propias fotos, y otra distinta, que suba fotos a las redes sociales de terceras personas. Esta situación puede conllevar que el usuario que inicialmente no estaba en una red social, acabe dándose de alta con la finalidad de para controlar o fiscalizar la información que se publica en las mismas sobre su persona, es decir, las fotos. No es lo mismo la publicación de fotografías captadas durante la realización de un congreso, que aquellas que se obtienen durante una cena entre amigos, en la que se muestre un comportamiento más bien desinhibido[26]. No nos hemos de olvidar tampoco del famoso etiquetado de las fotos en Facebook, lo que puede implicar que la divulgación de las

23 Para ver esta diferenciación, el concepto y clases de redes sociales puede verse: Campuzano Tomé, H. (2011). Las redes sociales digitales: concepto, clases y problemática jurídica que plantean en los albores del siglo XXI. *Actualidad Civil.* Nº. 1.

24 Moreno Navarrete, M.A. (2010). Aspectos jurídico privados de las tecnologías Web 2.0 y su repercusión en el derecho a la intimidad. En Javier Boix Reig (Dir.) y Ángeles Jareño Leal (Coord.), *La protección jurídica de la intimidad.* Madrid: Iustel, p. 346 y 347. Así lo pone de manifiesto este autor al hablar de los riesgos que entrañan las redes sociales de forma gráfica, al entender que «los riesgos visibles son solo la punta del iceberg» y que «En este sentido, los usuarios de forma conjunta delimitan su perfil como grupo e individualmente, lo que supone una amenaza más que por la cesión de datos, que es su antesala, a los derechos de la personalidad, como la intimidad y la propia imagen».

25 Faerman, J. (2010). *Faceboom. Faceb*o*k, el nuevo fenómeno de masas.* Argentina: Alienta editorial, p. 86.

26 Son numerosos los casos del impacto negativo que ha tenido la publicación de una foto captada dentro de un contexto social, o entre amigos, y su rápida divulgación en Internet y las redes sociales. El último ejemplo ha sido el de un ex edil de la población de Nules que ha tenido que dejar su

mismas pueda ser mayor. Este tema plantea determinados problemas jurídicos respecto al consentimiento para la publicación de las fotografías, que será analizado en un epígrafe posterior[27].

Internet y las redes sociales son accesibles fácilmente a cualquier usuario. Por tanto, el impacto que pueda tener la publicación de una fotografía puede ser mayor que el que tenga en los medios de comunicación tradicionales, ya que los usuarios de Internet son «potenciales usuarios». Es decir, la captación y publicación de una fotografía de un personaje famoso en una revista, de la denominada prensa rosa, será vista por las personas que la compren. Ello no ocurre en Internet. El daño que se puede causar o el impacto que pueda tener es mayor, dada la rapidez con la que la información se va transmitiendo entre usuarios. Por otro lado, como ha puesto de relieve la doctrina, las redes sociales se basan en lo que se denomina «la teoría de los seis grados de separación», propuesta por el sociólogo Duncan Watts en su libro «*Six Degrees: The Science of a Connected Age*». Moreno Navarrete explica muy bien en qué consiste la misma: «*cualquier individuo puede estar conectado a cualquier otra persona en el planeta, a través de una cadena de conocidos con no más de cinco intermediarios (con un total de seis conexiones). La cifra de conocidos aumenta a medida que lo hacen los eslabones de la cadena. Los individuos de primer grado serán los más próximos y, según se avanza en el grado de separación, disminuye la relación y la confianza*»[28].

Por otro lado, como ya se ha destacado, la LO 1/1982 tiene más de 30 años, por tanto, en la mente del legislador ni se le hubiera pasado por la cabeza el desarrollo, impacto y las implicaciones para la sociedad que tendría Internet y las redes sociales en los años posteriores. A este respecto, De Miguel Asensio ha señalado que «pese a la profunda transformación que en este ámbito ha supuesto la expansión del uso de los servicios de la sociedad de la información; con carácter general, la circunstancia de que la intromisión en el derecho al honor, a la intimidad y a la propia imagen se lleve a cabo a través de Internet (típicamente, por ser el medio empleado para la divulgación de hechos o expresiones, la revelación de datos y la utilización o publicación de imágenes o nombres) no altera desde el punto de vista material o sustantivo los criterios determinantes en nuestro ordenamiento para apreciar la existencia de una intromisión ilegítima en los términos del artículo 7 LO 1/1982, ni modifica el contenido de estos derechos ni su ponderación con otros derechos fundamentales, ámbito en el que resulta clave la labor de interpretación del TEDH y del TC» [29].

---

cargo al publicarse una foto en la que simulaba que estaba preparando rayas de cocaína. http://www.20minutos.es/noticia/2118763/0/jose-vicente-adsuara/concejal-nules/dimite-cocaina-coca/

27 Epígrafe 3.2.

28 Moreno Navarrete, M.A. (2010). *Aspectos jurídico privados…, op.cit,* p. 340.

29 De Miguel Asensio, P.A. (2010). *Derecho privado de Internet,* Navarra: Thomson Aranzadi, p. 164.

Esta ley se ha aplicado a aquellos supuestos de vulneraciones del derecho a la propia imagen en los medios de comunicación tradicionales, sobre todo en el ámbito de la denominada prensa rosa y en relación con personajes públicos. En la actualidad, los tribunales están resolviendo algunos casos relacionados con las redes sociales y las publicaciones en Internet, pero se centran básicamente, dejando a un lado la protección de datos, en las lesiones en el derecho al honor o a la intimidad. Son escasos los que hay, hasta el momento, de vulneración al derecho a la propia imagen de personas anónimas en las redes sociales o Internet, aunque las que hay, como hemos comentado, normalmente van acompañadas de lesiones al honor de los afectados o de su dignidad y básicamente se centran en el ámbito del Derecho Penal por existir algún tipo de delito o falta. Por ejemplo, en la sentencia de la Audiencia Provincial de Córdoba de 26 de febrero de 2009[30] se considera que *«la mera publicación de una fotografía de grupo en la que aparece la denunciante en una actitud correcta y con una imagen que en ningún caso es ofensiva o denigratoria no puede considerarse constitutiva de vejaciones injustas, sin perjuicio del alcance que dicha actuación pudiera tener sobre el derecho a la intimidad o a la propia imagen en la esfera civil»*. En este caso la publicación de la foto iba acompañada de comentarios de mal gusto, los cuales el tribunal consideró que no eran constitutivos de infracción penal, *«sin perjuicio de su posible ilicitud civil, por atentar a los derechos fundamentales al honor, a la intimidad y a la propia imagen»*. La sentencia de la Audiencia Provincial de Valencia de 20 de enero de 2009[31] condena a un año de prisión a un señor que se estaba separando de su mujer, por crear una página web en la que colgó varias fotos de su mujer y sus hijas, con determinados comentarios que podíamos calificar de mal gusto. En el orden civil, en el caso de la sentencia de la Audiencia Provincial de Valencia de 9 de abril de 2003[32] se consideró que existía intromisión ilegítima en el derecho a la intimidad y a la propia imagen porque se habría producido la divulgación de la fotografía del demandante haciendo *puenting* tanto en un cartel como en la página web correspondiente, reconociéndole una indemnización de 3.200 euros.

3.2. El problema del consentimiento en el marco de Internet y las redes sociales

Como se dijo anteriormente, uno de los elementos para excluir la intromisión ilegítima en el derecho a la propia imagen es el consentimiento del afectado. Dicho consentimiento emitido para hacerse una fotografía no se hace extensivo a su divulgación o publicación ya que «*es preciso el consentimiento específico para cada acto de injerencia en el derecho a la propia imagen de una persona y, más específicamente aún, el consentimiento a*

30 JUR 2009\322889.

31 JUR 2010\181056.

32 JUR 2003\171166.

la publicación»[33]. Se señaló también que la LO 1/1982 habla de consentimiento expreso, pero la jurisprudencia ha entendido que hacer un posado es una forma de manifestación del consentimiento[34]. La doctrina considera que no hace falta que sea escrito, puede ser verbal y que cuando se habla de consentimiento expreso «*significa consentimiento específico y determinado para una concreta intromisión en la propia imagen, que puede alcanzar (…) al medio con que se capta y donde se publica. Expreso sería sinónimo de intencionado, preciso o concreto, de manera que la norma estaría prohibiendo un consentimiento genérico o indeterminado, impreciso o ambiguo*»[35]. No obstante, si este tema, en los medios de comunicación tradicionales, es difuso, en Internet y las redes sociales se agrava más la situación, y a dicha confusión no ayuda que el art. 2.1 de la norma señale que «*La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia*». ¿Cómo interpretamos este precepto en su aplicación en las redes sociales?

Supongamos la siguiente situación: salimos a cenar con los compañeros del trabajo. Uno de ellos, usuario asiduo y frecuente de las redes sociales, capta las imágenes de la cena. Este sujeto suele colgar en Facebook todas las fotografías que realiza y nosotros somos conocedores de este hecho. Si no le manifestamos nuestro desacuerdo con que publique aquellas fotos en las que aparecemos, ¿estamos dando el consentimiento tácito, por tanto, para que las publique aunque la ley hable de consentimiento expreso? ¿Si dejamos que el usuario de una red social cuelgue fotos nuestras una vez, implica que le estamos dando el consentimiento para que posteriormente lo haga con todas las fotos que vaya captando? Y si no le damos el consentimiento ¿cómo

33 Castilla Barea, M. (2011.) *Las intromisiones legítimas..., op.cit.,* 149.

34 La sentencia básica en esta materia es la STS de 3 de noviembre de 1988 (RJ 1988\8408), cuyo fundamento de derecho segundo, si bien es breve manifiesta lo siguiente: *«En íntima relación con el motivo anterior se articula el segundo denunciando, bajo el amparo de la causa quinta del artículo 1692 de la Ley de Enjuiciamiento Civil la infracción del artículo 1253 del Código Civil con la engañosa argumentación, de que estando la imagen de la fotografía en una clara posición de posar, lleva necesariamente a la convicción de que la actora dio su consentimiento al fotógrafo para la obtención de la misma por lo que debió aplicarse dicho artículo al existir entre ambos hechos -posición de posar y consentimiento- un enlace preciso y directo; y si es así, respecto en cuanto a ser «fotografiada» se refiere, no cabe sentar la misma deducción en cuanto a su publicación, para lo que preciso se hace, contar con su expreso y concreto consentimiento, el que no cabe entender, aun llevando más allá aquella vía presuntiva, concedido de modo implícito dado los términos en los que aparece redactado el apartado 2 del artículo 2.º de la Ley de 5 de mayo de 1982 (…)».*

35 Blasco Gascó, F.de P. (2008). *Patrimonialidad y personalidad de la imagen.* Barcelona: Bosch, p. 132. Sin embargo, la doctrina ha puesto de manifiesto la dificultad existente en determinar cuándo un consentimiento es expreso, presunto o tácito. Castilla Barea, M. (2011). *Las intromisiones legítimas..., op.cit.,* pp. 169 y ss.

podemos verificar si le decimos a esa persona que no publique nuestras fotos que realmente no lo ha hecho? ¿O cómo podemos evitar que las cuelgue? Estos son algunos interrogantes que hemos de plantearnos en la práctica. Lo idóneo sería que el sujeto afectado, al tener conocimiento que van a ser colgadas determinadas fotos suyas, se manifestara sobre su autorización para su publicación. Pero el problema esencial es determinar qué medios tendría a su alcance el afectado para evitar esta conducta. Con el tenor literal de la ley, y en concreto, con el art. 2.2 LO 1/1982, la publicación de fotografías en una red social o en Internet sin nuestro consentimiento será una intromisión ilegítima, con independencia que produzca o no un daño como veremos en el apartado posterior.

Lo que hemos de tener presente es que si damos el consentimiento para la publicación de determinadas fotos en una red social, en un momento concreto, no implica que estemos concediendo un consentimiento genérico para cualquier acto de difusión o de publicación en las redes sociales de cualquier fotografía que pueda captarse nuestra. Algunos autores han intentado dar alguna propuesta de solución cuando alguien cuelga, por ejemplo, fotos sin nuestro consentimiento o no se cuenta con el consentimiento de todos los afectados. Una de las soluciones pasaría por pixelar los rostros de las personas[36]. Si bien hoy en día ésta puede ser una solución, consideramos que puede haber un abanico más amplio de respuestas a los problemas que se planteen. De ahí que sean los tribunales los que vayan resolviendo estas cuestiones a medida que se les vayan presentando las intromisiones ilegítimas en el derecho a la propia imagen en las redes sociales.

3.3. Referencia a la captación, reproducción y publicación de las fotografías en las redes sociales y la causación de daño

Cuando un usuario capta, difunde o publica fotografías de determinadas personas, en Internet o en las redes sociales, la casuística que puede presentarse en relación con la posible causación de un daño es diversa. Podemos encontrarnos, por ejemplo, que la difusión o publicación de una fotografía de una persona sin su consentimiento y su posterior publicación en una red social, no provoque ningún daño al sujeto en cuestión[37]. Pongamos por ejemplo, la publicación de una foto tomada en una reunión donde la persona fotografiada, un personaje no público, está hablando con otra persona, en actitud normal. En principio, esta situación no tendría que provocarle ningún daño, con independencia de que la captación de la misma sin el consentimiento del titular se considere una intromisión ilegítima en su derecho a la propia imagen, por haberse tomado la foto

36 Soler Presas, A. (2011). Am I in Facebook? *Indret*, 3/2011, p. 36.

37 Es lo que la doctrina denomina como el «uso inocuo de la imagen de otro». Blasco Gascó, F.d.P. (2008). *Algunas cuestiones*…, *op.cit.,* p. 27.

y publicado sin su consentimiento[38], salvo que no concurra alguna causa que legitime la intromisión. Podemos encontrarnos también la situación en que la captación de la foto de una persona y su consiguiente publicación en las redes sociales le reporte un beneficio[39]. La última situación que puede darse, es que la captación y publicación, así como la difusión de la foto o imagen provoque un daño, básicamente moral, al sujeto afectado. Pongamos el caso de un político, al cual se le fotografía en una fiesta privada en estado de embriaguez o mostrando conductas poco ejemplares. La publicación y divulgación de esta fotografía, sin su consentimiento, puede provocarle un daño considerable, además, de afectar a otros derechos como el honor y la intimidad. O pongamos el caso de un fotomontaje realizado a una persona que además, puede vulnerar su honor. Como sabemos, Internet y las redes sociales son canales idóneos para que las mismas lleguen al máximo de usuarios posibles. Es decir, los «potenciales» receptores de dichas imágenes pueden ser infinitamente mayores que los receptores de la prensa escrita o los medios de comunicación, y por tanto, el daño será mucho mayor. El criterio de la difusión es uno de los criterios que se tienen en cuenta para cuantificar la indemnización. Así lo pone de manifiesto Atienza Navarro al señalar que «*El criterio de la difusión o audiencia, en los últimos tiempos, presenta un problema añadido que debe ser tenido en cuenta: las agresiones ilegítimas producidas mediante la moderna sociedad de la información, y, especialmente, a través de Internet. En esos casos, puede conseguirse, por ejemplo, que una imagen un sonido alcancen una difusión casi infinita. Lo peor es que, además, difícilmente funcionará la tutela inhibitoria o negatoria, ya que resulta imposible controlar el reenvío privado entre particulares*»[40].

En nuestro país parece que todavía no ha habido, al menos por el momento, casos en los que un fotomontaje, una caricatura o la publicación de una fotografía de una persona anónima haya provocado daños de entidad considerable, como sí ha ocurrido en otros países[41]. SOLOVE pone algunos ejemplos y el impacto que ha tenido el uso de la captación de la propia imagen de determinadas personas sin su consentimiento y

38 Atienza Navarro, M.L. (2011). Algunas cuestiones acerca de la responsabilidad civil por intromisiones ilegitimas en el derecho a la propia imagen. En José Ramón Verda y Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.141-165). Navarra: Thomson-Aranzadi, p. 148, pone precisamente de manifiesto esta situación es decir, la posibilidad de la existencia de una intromisión ilegítima pero que no provoque un daño indemnizable, por dos motivos: «a) porque el irrogado se repare de forma específica, y no mediante la indemnización de daños y perjuicios; b) porque no llegue a infringirse daño alguno (aunque esto es menos frecuente en la práctica)».

39 En la actualidad, podemos encontrarnos con diversos casos de personas anónimas que han llegado a convertirse en personajes famosos gracias a las redes sociales.

40 Atienza Navarro, M.L. (2011). *Algunas cuestiones…, op.cit.,* p. 164.

41 No así, respecto vídeos que han ido circulando a través por ejemplo de *Whatsapp*.

su publicación en Internet. Explica, entre otros, el caso de «*Little Fatty*», un estudiante chino al cual alguien tomó una foto y la subió a la red. Como consecuencia de sus rasgos físicos, empezaron a realizarse fotomontajes con su cara y el fenómeno fue tal, que dio la vuelta al mundo. O el caso de «*the dog poop girl*», una chica de Corea del Sur que se negó a recoger los excrementos de su perro en el metro. Alguien le hizo una foto y la subió a la red. Pues bien, a partir de ese momento la imagen empezó a difundirse y a realizarse diferentes fotomontajes. El impacto de este hecho fue tal que según cuenta el autor, la chica tuvo que abandonar la universidad [42]. ¿Qué hubiera ocurrido si esos casos se hubieran producido en nuestro país? En principio, hemos de tener presente que los derechos de la personalidad no son absolutos, y por tanto, pueden colisionar con otros, como el derecho a la libertad de expresión o información. Además, los derechos de las personas con proyección pública, como se ha reiterado por doctrina y jurisprudencia, quedan un poco más debilitados dada su condición, en «aras al interés general»[43]. ¿Pero una persona anónima o privada tendría que soportar la difusión sin su consentimiento de dichas fotos y fotomontajes en las redes sociales, con independencia que hayan realizado, (obviamente hablamos del caso de «*the dog poop girl*», no el de «*Little Fatty*») una conducta que puede ser reprochable socialmente? Según la LO 1/1982 la respuesta sería porque no podría encuadrarse en ninguno de los supuestos que hacen que la intromisión se considere legítima. Pero como hemos señalado, tendrán que ser los tribunales los que vayan resolviendo caso a caso los conflictos que se les vayan planteando.

4. CONCLUSIONES

La LO 1/1982 ha ido dando respuesta a las diversas lesiones del derecho a la propia imagen en el marco de los medios comunicación tradicionales. Sin embargo, Internet y las redes sociales están suponiendo un nuevo reto para la aplicación de esta ley, como consecuencia de diversos factores, entre ellos la rapidez con la que se difunde la información. Nuestros tribunales están resolviendo básicamente, conflictos relacionados con la protección de datos personales o la colisión del derecho al honor y los derechos a la libertad de expresión y de información. Por lo que respecta al derecho a la propia imagen, de momento no existen muchos casos relacionados con las intromisiones ilegítimas del mismo en las redes sociales, a no ser que vayan acompañados de lesiones a otros derechos, o puedan ser constitutivos de algún delito o falta. A pesar de los interrogantes

42 Solove, D.J. (2007). *The future of reputation: gossip, rumor, and privacy on the internet.* New Haven and London: Yale University, Press. El primer caso citado puede verse en las pp. 43 y ss., el segundo en las pp. 1 y ss.

43 O'Callaghan Muñoz, X. (1991). *Libertad de expresión...*, *op.cit.* p. 68 al hacer referencia al derecho al honor.

que se plantean en la actualidad, tendremos que esperar a ver cómo van resolviendo los tribunales, los distintos casos que se les vayan planteando para determinar si es necesario una reforma de la LO 1/1982 o es suficiente con una reinterpretación de la misma para dar cabida a esta nueva problemática.

5. BIBLIOGRAFÍA

Atienza Navarro, M.L. (2011). Algunas cuestiones acerca de la responsabilidad civil por intromisiones ilegitimas en el derecho a la propia imagen. En José Ramón Verda Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.141-165). Navarra: Thomson-Aranzadi.

Blasco Gascó, F. de P. (2008). *Patrimonialidad y personalidad de la imagen.* Barcelona: Bosch.

Blasco Gascó, F. de P. (2008). Algunas cuestiones del derecho a la propia imagen. *Bienes de la personalidad. XIII Jornadas de la Asociación de Profesores de Derecho Civil* (p. 13- 91). Murcia: Editum. Ediciones de la Universidad de Murcia.

Campuzano Tomé, H. (2011). Las redes sociales digitales: concepto, clases y problemática jurídica que plantean en los albores del siglo XXI. *Actualidad Civil.* Nº. 1.

Castilla Barea, M. (2011). *Las intromisiones legítimas en el Derecho a la Propia Imagen. Estudio de las circunstancias que legitiman la intromisión en la LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.* Navarra: Aranzadi.

De Miguel Asensio, P.A. (2010). *Derecho privado de Internet,* Navarra: Thomson Aranzadi.

De Verda y Beamonte, J.R. (2011). El derecho a la propia imagen en la Ley orgánica 1/1982, de 5 de mayo. En José Ramón Verda Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.41- 65). Navarra: Thomson-Aranzadi.

De Verda y Beamonte, E. y Soriano Martínez, E. (2011). El consentimiento como causa de exclusión de la ilegitimidad de la intromisión. En José Ramón Verda Beamonte (Coord.), *El derecho a la imagen desde todos los puntos de vista* (p.67- 85). Navarra: Thomson-Aranzadi.

De Verda y Beamonte, J.R. (2007). Las intromisiones legítimas en los derechos a la propia imagen y a la propia voz. Un estudio del art. 8.2 de la Ley Orgánica 1/1982, de 5 de mayo, a la luz de la reciente jurisprudencia. *Diario La Ley,* nº. 6754, Sección Doctrina, 11 de julio de 2007, Año XXVIII.

De Verda y Beamonte, J.R. (2007). «1955 SENTENCIA DE 7 DE MARZO DE 2006: Intromisión ilegítima en el derecho a la propia imagen. *Cuadernos Civitas de jurisprudencia civil,* nº. 73, 329-341.

Dumortier, F. (2009). Facebook y los riesgos de la «descontextualización» de la información. *Revista de Internet, Derecho y Política,* número 9, p. 32, http://journals.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier

Faerman, J (2010). *Faceboom. Facebook, el nuevo fenómeno de masas.* Argentina: Alienta editorial.

Grimalt Servera, P. (2007). *La protección civil de los derechos al honor, a la intimidad y a la propia imagen.* Madrid: Iustel.

Moreno Navarrete, M.A. (2010). Aspectos jurídico privados de las tecnologías Web 2.0 y su repercusión en el derecho a la intimidad. En Javier Boix Reig (Dir.) y Ángeles Jareño Leal (Coord.), *La protección jurídica de la intimidad.* (p.335-360) Madrid: Iustel.

O'Callaghan Muñoz, X. (1991). *Libertad de expresión y sus límites: honor, intimidad e imagen.* Madrid: EDERSA.

Ortiz López, P. (2013). Redes sociales: funcionamiento y tratamiento de información persona. En Artemi Rallo Lombarte y Ricard Martínez Martínez (editores), *Derecho y Redes Sociales* (p. 21-37). Navarra: Civitas y Thomson Reuters.

Soler Presas, A. (2011). Am I in Facebook? *Indret*, 3/2011

Solove, D.J. (2007). *The future of reputation: gossip, rumor, and privacy on the internet.* New Haven and London: Yale University, Press.

16

WHO WATCHES THE WATCHMEN? USE OF COOKIES ON MOST IMPORTANT SPANISH WEBSITES

Francisco José García Ull
Doctorando en Comunicación Universidad de Valencia / Heinrich Heine Universität Düsseldorf
Departamento de Teoría de los Lenguajes / Philosophische Fakultät

ABSTRACT: Since last March 2012, when the Spanish legislation incorporated the EU Directive on Electronic Privacy, all Spanish websites collecting users' data are required to inform clearly on the type and purpose of the data collected and to obtain the users' consent to use their data with analytic or marketing purposes. In order to provide support to webmasters, the Spanish Data Protection Agency (AEPD) released last April the «Use of cookies guidance» similar to the UK ICO «Guidance on the rules on use of cookies and similar technologies», with some advises to help websites accomplish with the current regulations. In October 2013, more than a year and a half after the law incorporation, the results of this research show that only 51% of the 500 most visited Spanish websites (according to Alexa Rank), apply the regulations correctly, asking their users for the informed consent to collect their data. As a direct consequence, a new question arises: Who are the trackers behind these cookies? We identify and analyze in this research the most important tracking corporations (also named Data Collectors) and their direct effect with Cyberspace Data Privacy. We propose, to complete the dissertation, the need for greater responsibility by stakeholders concerned, such as Institutions, Cybermedia and other relevant websites and Internet users. Internet users have the right to be correctly informed about the potential risks they assume while surfing the web and the right to know how these data will be used. As the boundaries between physical space and Cyberspace tend to disappear, E-privacy becomes a major issue, which has a direct effect not only in the online data safety, but also in the offline life.

KEYWORDS: e-Privacy, Cookies, Big Data, Behavioral Targeting, Advertising, Transparency.

1. INTRODUCTION

Last March 2012, Spanish legislation incorporated the EU e-Privacy Directive, also known as Cookie Law. The law requires all websites engaged in economic activities and collecting users' data through cookies or similar technologies to inform clearly on the type and purpose of the data collected and to obtain the users' consent. We consider interesting to see if, almost two years after the implementation of the regulations, the most visited websites in Spain correctly inform their users about their data collection, with statistical or marketing purposes. We also suggest the need for identify the most important data collection companies behind the cookies operating in Spain, in order to provide greater transparency on the Web. We believe data privacy of Internet users'

is one of the major challenges we face in the coming years. As the boundaries between physical space and cyberspace tend to disappear, privacy of Internet users becomes a matter of vital importance with also direct consequences in offline word data safety[1].

1.1. Internet usage in Spain

According to eEspaña 2013 report, developed by the Orange Foundation[2], 68% of Spanish households have an Internet connection and 25 million Spanish people used the Internet in 2012. Regarding the expansion of the Mobile Web, the statistics underline that 39% of Spanish people have used a laptop or mobile phone to access the Internet.

Most Web users in Spain use the Internet to send or receive emails, search for information and access to news and online media. Half of the Internet users make more complex activities such as participating in social networks or downloading content such as games, movies or music.

The figures state that, in general terms, Spanish citizens are above the European average in many uses of the Internet. Noteworthy in this regard a significant difference in the use of services related to entertainment and creativity. For example, while 45.6% of Spanish Internet users upload content on websites to be shared, in the rest of Europe this activity is only done by a third of the Internet users.

The data we observe, as well as the prospective studies, predict an increasingly ubiquitous Web, in an increasingly connected and Internet dependent society.

We could assume, in this sense, there is a risk of diving into the rivers of information without having the necessary tools to ensure our privacy. Technological progress, in our opinion, must be hand on hand with users' education and with the necessary mechanisms to ensure user's privacy, web transparency and, ultimately, a more democratic Web.

We would like to emphasize the need, which is the subject of this study, to evaluate the potential risks on data privacy Internet users assume while surfing the Web. It is important, in our point of view, to be aware of the lack of information in this area[3]. That is the main reason we have decided to observe the degree of compliance with data

---

1 Hodges, Dept. of Comput. Sci., Univ. of Oxford, Oxford, UK D.; Creese, S. (2013). Breaking the Arc: Risk control for Big Data. *IEEE Big Data 2013*, 613-621.

2 Fundación Orange (2013). *eEspaña 2013: informe anual sobre el desarrollo de la sociedad de la información en España.* Retrieved June, 5th, 2013 from http://www.proyectosfundacionorange.es/docs/eEspana_2013_web.pdf.

3 According to a research *The Impact of Cookie Deletion on Site-Server and Ad-Server* (2011) developed by the Web Analytics company Comscore, third party cookies are deleted monthly at a rate of between 30% and 40% of computers, depending on the country. This means that between 60% and 70% of Internet users do not remove cookies frequently.

protection regulations by most influent Spanish websites, as well as to identify the leading data collectors, which gather the information we generate while surfing the Web. We would like to believe this kind of studies can somehow help clarifying this complex scenario, while putting on the table some of the potential risks that we will undoubtedly have to face in the coming years.

1.2. Online Privacy and Legislation

In 2003 was implemented the European Directive 2002/58/EC[4] which aimed to protect users privacy in electronic communications. In 2009, it was amended by Directive 2009/136/EC[5], with a modification in the Article 5(3) of the e-Privacy Directive, which requires the consent to store or access to information stored in users' or subscribers' terminals. In other words: it is an essential requirement to obtain the consent of the Internet users to install cookies and similar technologies. European legislation started, since then, requiring the explicit or implied consent of the users, to websites using cookies that may threaten users' privacy.

The EU directive was incorporated into Spanish legislation on March 31st, 2012[6] and, in order to make compliance easier for websites, Spanish Data Protection Agency (AEPD) published last April 2013 the «Use of Cookies Guidance», developed in collaboration with media and advertising agencies.

The report, which is similar to the UK ICO «Guidance on the rules on use of cookies and similar technologies», offers advice on how to comply with e-Privacy regu-

4 European Union (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Official Journal L 201, 31st of July 2002, 0037-0047. Retrieved September, 11th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

5 European Union (2009). *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*. Retrieved September, 11th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

6 España. *Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista*. Boletín Oficial del Estado, 31st of March 2012, 78, 26876- 26967. Retrieved September, 11th, 2013 from http://www.boe.es/boe/dias/2012/03/31/pdfs/BOE-A-2012-4442.pdf.

lations. Basically, the document explains that all websites collecting users' data which are not strictly necessary for the correct function of the website, are required to clearly inform about the type and purpose of the data collected, and to obtain the consent of the users to exploit their data with analytic or advertising objectives.

According to the ICO Cookies Guidance[7], a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the next requirements are met:

a) The user is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

b) The user has given his or her consent.

Or, summarizing the above information, those setting cookies must:

a) Tell people that the cookies are there,

b) Explain what the cookies are doing, and

c) Obtain their consent to store a cookie on their device.

About a year and a half after the incorporation into Spanish legislation of the EU Directive, particularly in early July 2013, about half of Spain's most important cybermedia, did not apply correctly the law yet[8]. It is true, however, the adaptation of websites to the new EU guidelines, as has been shown for example by reports published by Discapnet on Web Accessibility, may take some time to implement.

It is necessary in this regard to underline that article 5, paragraph 3 of Directive 2002/58/EC, allows cookies to be exempted from the requirement of informed consent, if they satisfy one of the following criteria:

- Criterion a) the cookie is used «for the sole purpose of carrying out the transmission of a communication over an electronic communications network».
- Criterion b) the cookie is «strictly necessary in order to the provider of an information society service explicitly requested by the subscriber or user to provide the service».

Accordingly, the Working Group of Article 29, in its Opinion 04/2012 on Cookie Consent Exemption[9], concludes websites using these cookies are exempted to require their user's consent:

---

7 Information Commisioner's Office (ICO) (2012) *Guidance on the rules on use of cookies and similar Technologies*. Privacy and Electronic Communications Regulations. Retrieved September, 11th, 2013 fromhttp://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.

8 García-Ull, F.J. (2013): Las cookies en los principales cibermedios generalistas de España. *Miguel Hernández Communication Journal*, 4, 233-261.

9 Article 29 Data Protection Working Party (2012). Opinion 04/2012 on Cookie Consent Exemption, Adopted on 7th June 2012. Retrieved June, 5th, 2013 from http://ec.europa.

- «*User-input*» cookies
- Authentification cookies
- User centric security cookies
- Multimedia player session cookies
- Load balancing session cookies
- UI customization cookies (language preference cookies, result display preference cookies).
- Social plug-in content sharing cookies

On the other hand, among non-exempted cookies (the websites using these cookies are required to provide information and obtain users' consent) we can find:

- Social plug-in tracking cookies
- Third party advertising
- First party analytics

1.3. About cookies

The Regulations are applied to cookies and similar technologies used by websites to store information. This definition includes, for example, Local Shared Objects (commonly named «Flash Cookies») and web beacons (transparent 1x1 pixels images).

According to the website *All about* cookies, «Cookies are usually small text files, given ID tags that are stored on your computer's browser directory or program data subfolders. Cookies are created when you use your browser to visit a website that uses cookies to keep track of your movements within the site, help you resume where you left off, remember your registered login, theme selection, preferences, and other customization functions. The website stores a corresponding file(with same ID tag)to the one they set in your browser and in this file they can track and keep information on your movements within the site and any information you may have voluntarily given while visiting the website, such as email address. […] Cookies are often indispensable for websites that have huge databases, need logins, have customizable themes, other advanced features. However, marketing is becoming increasingly sophisticated and cookies in some cases can be agressively used to create a profile of your surfing habits».

Cookies can be classified into different categories in relation to their functions. It is important to underline that the same cookie may be included in more than one category.

---

eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

The next classification is based on the analysis made by the Spanish Data Protection Agency (AEPD) and published in the «Use of cookies guidance»[10].

1.3.1. Depending on the entity who manages the cookie:

a) First-party cookies

These cookies are sent to the user's computer from a computer or domain managed by the website editor.

b) Third-party cookies

Third party cookies are cookies served from a domain other than the page in which it is embedded. Third-party cookies are usually not strictly necessary for the user to visit a website, as they are usually linked to a different service from the one specifically requested by the user.

1.3.2. Depending on the time cookies remain active:

a) Session cookies:

These files are deleted when the user closes the browser, once the navigation is completed. The next time the user visits the website, he or she is not recognized and is treated as a new user, since there is no file in the browser enabling the site to know if the user has visited it previously.

b) Persistent cookies:

These cookies remain on the hard disk of the terminal until the user removes them or they expire. The duration of the cookie depends on how the file has been programmed by the developer. These cookies have the ability to authenticate the user account, so the user do not have to provide his or her account details each new visit, as well as various options for interface customization, such as language selection, menu preferences, etc. The time these cookies remain on user's terminal can range from a few minutes to several years.

1.3.3. According to its purpose:

a) Technical cookies

These cookies allow the users to navigate and interact with the website.

b) Customization cookies:

10 Spanish Data Protection Agency (AEPD) (2013). *Guía sobre el uso de las cookies*. Retrieved June, 5th, 2013 from http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf.

Customization cookies allow users to access the service with some particular features based on a predefined set of criteria in the user terminal such as the language, the type of browser, font size, etc.

c) Analytics cookies

These cookies allow the website owner to monitor and analyze the audiences and the users' behavior in the site.

d) Advertising cookies:

These cookies allow web editors and online advertising companies to manage ad spaces in an efficient way.

e) Behavioral targeting cookies:

These cookies store information about users' behavior. These data are obtained through a continued observation of users' browsing habits. The information collected makes possible to develop a specific profile of each user and to display ads based on his or her preferences.

2. METHODS

2.1. Universe of Study

We have selected in this study the top 500 websites in Spain, according to Alexa Rank, in September, 2013.

Alexa Internet, Inc. is a subsidiary company of Amazon, which has been established as one of the most important web audiences' measurement systems, auditing more than 30 million websites worldwide. Alexa Rank measures the popularity of websites throughout the cyberspace and offers the possibility to segment audiences by country. The rank is calculated using a combination of the estimated average daily unique visitors to the site and the estimated number of pageviews on the site over the past 3 months. The site with the highest combination of unique visitors and pageviews is ranked #1.

We have removed from the sample a total of 39 web addresses which, in our opinion, could decrease the reliability of the study, based on two reasons:

a) Duplicated addresses (27):

Like, for example, multiple extensions (http://www.google.de, http://www.google.fr, etc.), subpages (http://www.files.wordpress.com) or websites from the same owner (for instance, http://www.bookryanair.com).

b) URL addresses without a website (12):

We have removed here from the sample the URLs with redirections to other domains, or web addresses with marketing and tracking purposes, which do not lead to a website (for example, http://www.itrack.it).

The units analyzed after this filter are, therefore, a total of 461.

2.2. Analysis variables

2.2.1. Degree of compliance

The first objective of this research is to see if most important Spanish websites correctly apply the guidelines on privacy to comply with regulations concerning the use of cookies.

In order to develop this part of the study, we have analyzed the most popular websites in Spain according to Alexa Rank. In this regard we have considered appropriate at first discern the number of cookies used by each website, if they are first or third-party cookies and if the cookies are or not strictly necessary to use the service.

Cookies	Results
First-party cookies	0
Third-party cookies	0
Total	0
Strictly necessary	Yes/No

We have visited the top 500 Spanish websites with each one of the most used web browsers: Internet Explorer v.10, Google Chrome v.28 and Mozilla Firefox v.22.0.

If the website uses cookies which are not strictly necessary to provide the service required by the user, we have analyzed the two variables mentioned in the Spanish regulations:

a) Information: the website has to inform their users clearly about the use and purpose of the data collected.

b) Consent: after providing the information, the user must agree the data collection.

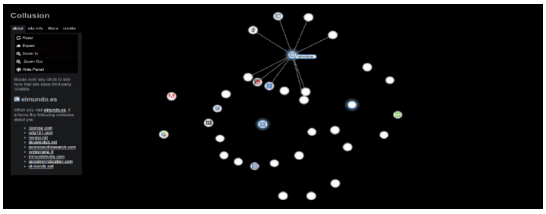
It is important to highlight among 500 most popular websites in Spain, there are a lot of companies and institutions established outside the Spanish and EU boundaries and, therefore, the Spanish legislation does not apply. As a consequence, we have selected from the universe of study those companies and institutions which, as indicated in the «Law of Information Society Services and Electronic Commerce» (LSSI) (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico)[11], have a perma-

11 España. Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. *Boletín Oficial del Estado*, 12 de julio de 2002, núm. 166, pp. 25388-25403. Retrieved July, 10th, 2013 from: http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf.

nent establishment in Spain. We have divided this part of the research into six different categories: Internet services, news, businesses, government agencies, online shops and websites with content for adults.

2.2.2. Most used cookies by top Spanish websites

On this second point we have used Mozilla Collusion tool to draw a map of cookies, web beacons and similar technologies used by most visited Spanish websites. We have also used Google Chrome's Ghostery tool to double check the data reliability.



Picture 1. Mozilla Collusion Interface

In this section we have considered convenient to analyze the 500 top Spanish websites provided by Alexa Rank (461 after the filter already mentioned), regardless of the companies or institutions nationalities. In our opinion, as they are the most visited platforms in Spain, the chances these cookies are installed on Spanish Internet users' web browsers are very high. The main objective of this part is to detect and identify the most important Data Collectors operating in Spain.

2.2.3. Most important Data Collectors in Spain

The third part of the study is based on the analysis conducted by The Guardian: *Tracking the trackers: who are the companies monitoring us online?*[12], developed with the help of its readers, in April 2012. The research, which collects information on more than 7000 websites, aims to identify the main companies that benefit from the information generated by Internet users' behavior on the Web.

In our case, we have used the tool Mozilla Collusion to analyze the 461 most visited websites by Spanish people, in several waves during the month of September 2013. After identifying the third-companies or Data Collectors, we have managed the

12 CROSS, Chris; GEARY, Joanna; (2012) *Tracking the trackers: who are the companies monitoring us online?* Battle for Internet. The Guardian, 23th of April, 2012. Retrieved September, 16th, 2013 from: http://www.theguardian.com/technology/interactive/2012/apr/23/tracking-trackers-companies-following-online.

data provided to discern how many websites among analyzed use a specific cookie, thus providing statistical information on cookies most used in Spanish cyberspace.

In the next step, we have created a detailed list of the main companies collecting data from the user's behavior, and tried to answer the following questions:

a) What is it? Which is the company responsible for the cookie?
b) What information does it collect?
c) Are data associated to personal information could identify a concrete user?
d) How long are data stored?
e) Are data sold to third parties?

3. RESULTS

3.1. Degree of compliance

Once established the top 500 most visited Spanish websites and, after performing the filter that we talked about in the methodology (eliminating duplications and ad tracking URLs), the sample is reduced to 461 websites.

Then we have observed the origin of each website to find out if whether or not they are established in Spain. Understandably, we have ignored in this analysis websites that, although very visited by Spanish people, are outside the scope of EU and national legislation.

According to the information obtained, we can highlight a first data: among the most visited websites by Spanish users, only 59% (272) are within the scope of Spanish legislation. The remaining 41% (189 websites, most of them from the U.S.) do not have, according to the current legislations[13], any legal obligation to require the informed consent to their users.

We have deleted from the universe of study those websites outside the scope of Spanish legislation. As a consequence, we have observed the degree of compliance focusing the analysis on the remaining 272 websites, which need to require informed consent to their users.

The result of the analysis show that 139 of the 272 pages we have tested (51%) correctly apply current legislation on privacy, while 133 (49%) of the analyzed websites do not apply the regulations and do not ask, when it is needed, for the informed consent to their users.

13 As stipulated in the LSSI, Spanish legislation will apply to service providers established in Spain. The company address in Spain must be indicated on their website and has to be able to be checked through Spanish Commerce Register. Spanish law also applies to purchases made to service providers established in another Member States of the European Union or the European Economic Area (EU countries plus Norway, Iceland and Liechtenstein).

At this point, we would like to highlight the fact that most of the 133 Spanish websites which do not apply the regulations, do it because they do not ask for the user's consent to use their data, although they provide information about cookies. In fact, 70% of analyzed websites that do not comply with the legislation, provide some kind of information about privacy and data protection to their users.

3.1.1. Degree of compliance classified in categories

We have divided the sample into 6 categories:

a) Internet Services (127 websites)
b) News (66 websites)
c) Businesses (34 websites)
d) Government agencies (24 websites)
e) Online shops (15 websites)
f) Adults (6 websites)

a) Internet services

We have selected in the *Internet Services* category those websites whose products or services are intrinsic to the nature of the Web, like weblogs, hypertext directories, search engines, forums, social network services, marketplace platforms, services based on the Web (like cloud computing) and other. The results show that 72 of the 127 websites analyzed (57%) do not comply with Spanish legislation. On the other hand, 55 websites (43%) correctly apply the legislations.

b) News

Online media use more cookies in average than the rest of websites. This should not be surprising, since the most important cybermedia's source of revenue is advertising and most of online web metrics and advertising techniques are based on the use of first and third-party cookies. Most visited Spanish websites install an average of 28 cookies in their visitor's devices (11 first-party and 17 third-party cookies). Most visited Spanish online media, on the other hand, install an average of 54 cookies (14 first-party and 40 third-party cookies). It stands to reason that digital media are more likely to threaten the Internet users' privacy, so we consider that this category is of particular importance.

According to the results of this research, 62% of the most important Spanish digital media correctly apply the current regulations. There is a 38%, however, do not require the informed consent to their users and, as a consequence, do not comply with the law yet.

c) Businesses

Within the most important corporate websites we have analyzed, we can find i.e. airlines, banks and IT companies. 50% of top business websites in Spain do not apply the e-privacy regulations while 50% correctly inform their users and ask for their consent to collect data.

d) Government agencies

Most of Spanish Government sites do not perform any economic activity and accordingly, do not need to ask for the informed consent to their visitors to collect their data[14]. However, there are some government platforms that use non-exempt cookies and provide products or services trough their websites (via, i.e. an online shop). These sites consequently, are required to comply with the obligations stipulated in the LSSI. There are 24 government websites within the top 500 most visited websites in Spain according to Alexa Rank. 83% of these websites (20) are not involved in any economic activity, so do not need to provide the informed consent to their users. On the other hand, 17% of these government platforms sell products or services online and use non-exempted cookies. However these websites do not correctly inform their users, and do not require the users' consent to collect their data, so we have to conclude they do not comply with the law.

e) Online shops

We have considered online shop in this research those platforms that allow users to buy products or services online and meet the characteristics inherent to this type of format (i.e. the shopping cart option). We have analyzed 15 sites within this category, including online shops from different industry sectors such as textile, furniture and decoration, food and entertainment. The results show that 67% of the analyzed samples do not apply correctly the regulations, while 33% precisely inform their visitors and customers and ask for their consent to collect data.

f) Adults

We have identified in this study 6 websites with content for adults within the scope of Spanish legislation. Only 1 of those websites (17%) complies with regulations, while the rest (83%) do not.

14 Spanish government agencies and administrations hardly ever have the need to require the informed consent to their users. This is because these websites are normally not involved in any economic activity (such as e-commerce or advertising). As stipulated in the LSSI if no economic activity is performed in the website, there is no need to ask for the informed consent to the users.

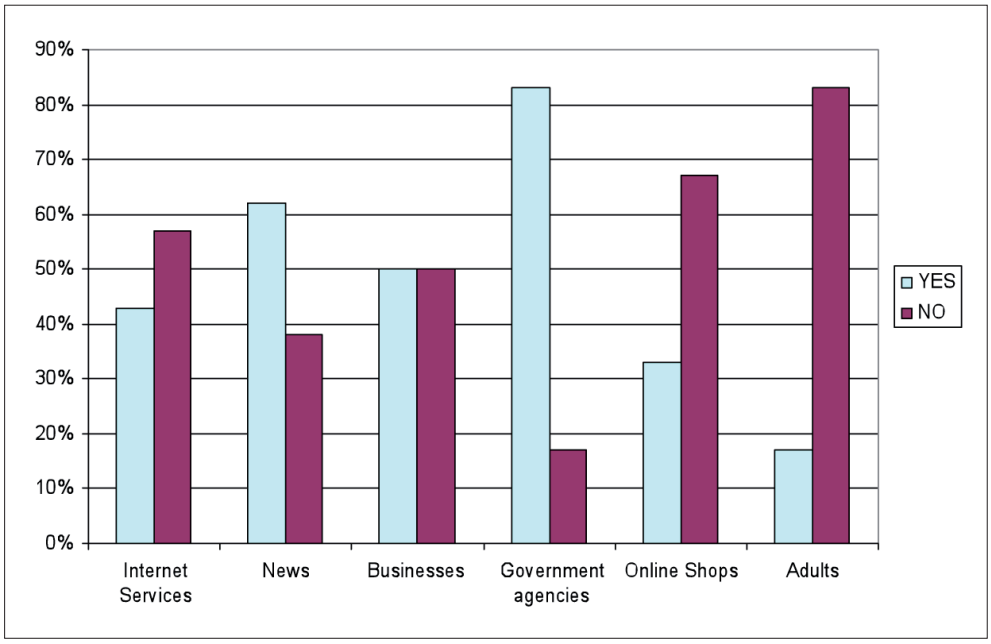


Figure 1. Most visited Spanish websites and compliance with Cookie Law

3.1.2. Most used cookies by top Spanish websites

With the help of Collusion tool we have generated a map of most frequently used cookies and similar technologies in Spanish websites. There is a high probability, thereby, any Internet user in Spain have some of the following cookies installed in their devices once the navigation is completed.

As mentioned, after filtering the 500 most visited Spanish websites according to set criteria (duplications and ad tracking URLs), the sample is reduced to 461 websites.

Collusion tool detects a total amount of 882 different cookies and similar technologies. In other words, after visiting the 461 most relevant sites in Spain within the same navigation session, the information generated while browsing the Internet is collected by 882 different cookies. These files send the data collected to the companies responsible of their installation and they will be frequently used with commercial or statistical purposes.

The most commonly used cookie is, by far, Google Analytics cookie –google-analytics.com–. It is followed by DobleClick cookie –doubleclick.net– (which is an online advertising company owned by Google), Facebook –facebook.com cookie–, comScore –scorecardresearch.com web beacon– and AppNexus –adnxs.xom cookie–.

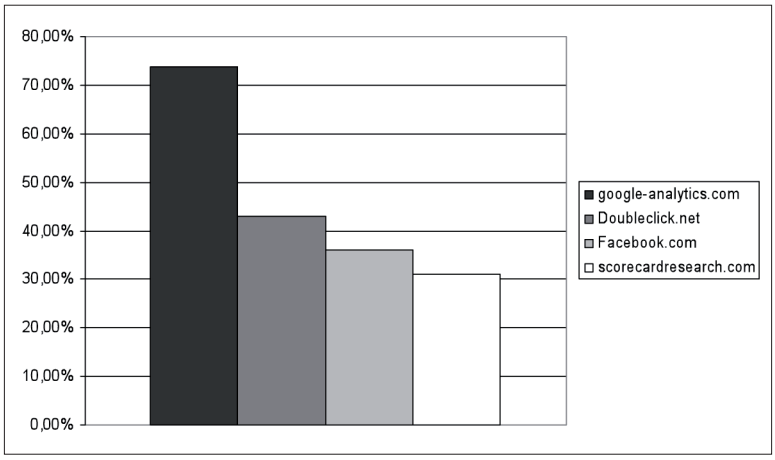


Figure 2. Most used cookies by top websites in Spain

We identify below the list of 50 most used cookies in most visited websites in Spain (Table 1).

Rank	Cookie name	Number of websites	Percentage
1	google-analytics.com	340	73,75%
2	Doubleclick.net	198	42,95%
3	Facebook.com	166	36,01%
4	scorecardresearch.com	143	31,02%
5	google.com	109	23,64%
6	googlesyndication.com	68	14,75%
7	ajax.googleapis.com	59	12,80%
8	fonts.googleapis.com	52	11,28%
9	google.es	49	10,63%
10	adnxs.com	46	9,98%
11	twitter.com	45	9,76%
12	serving-sys.com	42	9,11%
13	imrworldwide.com	40	8,68%
14	Factbook.net	34	7,38%
15	googleadservices.com	34	7,38%
16	Quantserve.com	29	6,29%
17	googletagmanager.com	27	5,86%
18	cxense.com	25	5,42%
19	youtube.com	25	5,42%
20	Chartbeat.net	23	4,99%
21	Xiti.com	23	4,99%
22	2mdn.net	22	4,77%

Rank	Cookie name	Number of websites	Percentage
23	smartadserver.com	22	4,77%
24	criteo.com	21	4,56%
25	gstatic.com	21	4,56%
26	wtp101.com	21	4,56%
27	2o7.net	20	4,34%
28	twimg.com	20	4,34%
29	omtrdc.net	19	4,12%
30	yieldmanager.com	19	4,12%
31	atemda.com	16	3,47%
32	dnn506yrbagrg.cloudfront.net	16	3,47%
33	newrelic.com	16	3,47%
34	Rubiconproject.com	16	3,47%
35	Weborama.fr	15	3,25%
36	bluekai.com	13	2,82%
37	sascdn.com	13	2,82%
38	360yield.com	12	2,60%
39	adroll.com	12	2,60%
40	betrad.com	12	2,60%
41	d5nxst8fruw4z.cloudfront.net	12	2,60%
42	disqus.com	12	2,60%
43	mathtag.com	12	2,60%
44	optimizely.com	12	2,60%
45	Uservoice.com	11	2,39%
46	gigya.com	10	2,17%
47	ivwbox.de	10	2,17%
48	revsci.net	10	2,17%
49	247realmedia.com	9	1,95%
50	atdmt.com	9	1,95%

Table 1. Most used cookies by top websites in Spain

As we can see in the chart above, 73.75% of most visited Spanish websites use Google Analytics cookie, 42.95% use DoubleClick Advertising cookie, 36.01% use Facebook cookie and 31.02% use comScore online audience measurement web beacon.

3.1.3. Most important Data Collectors in Spain

This classification is based on the *Tracking the Trackers* project, developed by The Guardian, in cooperation with its readers. We have also individually analyzed the information provided on each Data Collector's websites. We have selected at this point those

companies whose cookies are most frequently used in top Spanish websites: Google, DoubleClick, Facebook and comScore.

a) Google Analytics

What is it?

Google Analytics is a free tool that can be used by website publishers to better understand how people are using their website. It is also used by Google to better understand the performance of its own websites.

What information does it collect?

According to The Guardian study, Google Analytics cookie stores a unique identifier –so the website can recognize the user if he or she visits the website again– as well as information about the pages the browser visits; when the browser is seen on the website; how long the browser was seen on the website; the IP address (which can allow the Google Analytics to infer the browser's location), and what site the browser was looking at before arriving at the site (the referring url).

By default, this information is shown to website publishers through the Google Analytics tools and is not shared with anyone else. It is a first-party cookie.

Are data associated to personal information could identify a concrete user?

Data collected are not associated to any personal information according to Google.

How long are data stored?

If the user does not delete the cookies, Google Analytics cookies expire after two years.

Are data sold to third parties?

Websites may share anonymous analytics data with Google and other companies.

b) Doubleclick

What is it?

Doubleclick is a company owned by Google which business model is based on two sides: online advertisers and publishers. The business operates in tree different branches:

1. Ad-serving: Online publishers use Doubleclick to display adverts on their websites.
2. Ad delivery: Doubleclick let advertisers control how often an ad is shown to a browser, how long it is shown for and how often it will appear.
3. Behavioural targeting It is divided in two categories:
    a) Targeting for one website owner: an online publisher can set a Doubleclick cookie to identify the users' favorite sections on the website. Doubleclick will then select the type of adverts the users might like to see according to the browsing information collected. For example, if the user visits the sports pa-

ges of a news website, then adverts for match tickets may be more relevant. This information belongs to the website owner only.

b) Targeting in advertising networks: Google runs a service called Adsense, in which lots of different publishers pool the information they get on browsers. This helps them build up a better idea of the type of adverts someone might want to see. This is a third-party advertising cookie.

What information does it collect?

In their privacy policy, Google explains how data is recorded from a generic Doubleclick cookie. It looks like this:

time: 06/Aug/2013 12:01:32
ad_placement_id: 105
ad_id: 1003
userid: 0000000000000001
client_ip: 123.45.67.89
referral_url: «http://youtube.com/categories»

This data send Doubleclick information about the time and date the user see an advert. It also shows:

userid: the unique ID number the cookie has given user's browser
ad_id: the unique ID of the advert
ad_placement_id: the ID of where the advert was seen on the site
referral_url: what page the user was on when he or she saw the advert

Doubleclick can also collect user's geolocation information via IP address.

Are data associated to personal information could identify a concrete user?

According to Google, data are never associated to any personal information. This would be a breach of Doubleclick's terms and conditions. The information obtained from the cookies is never combined with information that Google obtains from its other products and services. Users' browsing behaviour will never be linked to users' Gmail accounts, for example.

How long are data stored?

Doubleclick cookies on the browser are set to expire after a number of years. However, the override for this is clearing cookies. Newer cookies «60 days in market» and «30 days in market» are actually more valuable to advertisers as they give a better indication of what the person using that browser is interested in right now. IP addresses are anonymized after nine months and the data in cookies is anonymized after 18 months.

Are data sold to third parties?

According to Google and, as highlighted by The Guardian, data are not sold to third parties. When the service is being used by a publisher for its own purposes (not in an ad network), the publisher owns that data, not Doubleclick.

c) Facebook

What is it?

Facebook is the most used social network on the Internet. Facebook has been estimated an average of 750 million unique visitors per month in 2013. It is followed in the same category by Twitter, with 250 million unique visitors per month, and Linkedin with 110 million.

What information does it collect?

The Facebook tracker that appears in our data is not for targeted advertising. In fact, Facebook explicitly told The Guardian researchers it has no need for such a thing – the information its users willingly volunteer on the platform is a far richer resource for advertising.

Facebook's cookies installed in user's devices are frequently related to the Facebook's «social plugins». These are tools that link back to Facebook in some way, such as the «like», subscribe» or «recommend» buttons.

They appear on other websites through the use of «iframes», a very common way of embedding content on to a web page. In order for this to load, Facebook's servers will know the page, the time and date it was loaded and the browser IP address.

Facebook's tracking cookies are used in three different ways:

1. If the user does not have a Facebook account and his or her browser has loaded a facebook.com page, then no cookie is set when the user browses a page with social plugins.
2. If the user does not have a Facebook account but has visited a facebook.com page in the past, three cookies are installed. One is for security reasons and the other two are used to track registration effectiveness. If a user later decides to create an account, the aim is to find out what convinced them to do it. This is done by recording the first and last Facebook pages the browser visited.
3. If the user has a Facebook account, a cookie is set on the browser containing a unique ID that relates back to the user's profile. When the user visits a page with a social plugin, it will check that cookie. If the user is signed in, it will use a unique ID to show you how many of the user's contacts in the social network have clicked on the like button and whether or not you the user has liked the page.

Are data associated to personal information could identify a concrete user?

If the user clicks on a Facebook «like» or «share» button, this is displayed on the user's Facebook wall. In order to do this, Facebook has to match this action with the user's account details. This is done through the log-in cookie.

How long are data stored?

Data associated with a user's Facebook account is stored for as long as that account is active. When the user deletes an account, it is permanently removed from Facebook.

It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days.

Are data sold to third parties?

Information about the social plugins the user has clicked will be shown to his or her friends, both on Facebook or on the. Facebook says these information is not shared with anyone else.

d) comScore

What is it?

ScorecardResearch is part of a company called Full Circle Studies, which is owned by comScore. comsCore tracks more than three million unique websites worldwide and its methodology page says it has «approximately two million worldwide consumers under continuous measurement».[15] It provides market research data to website owners through a mixture of online surveys and the use of web beacons[16].

What information does it collect?

ScorecardResearch's privacy policy says its tracking will collect information such as: when a browser visited a website, what page of the website it was, the title of the web page or the IP address.

Are data associated to personal information could identify a concrete user?

As with all cookies and web beacons, ScorecardResearch cannot identify an individual user who is using the computer to visit a website that contains a ScorecardResearch tag.

However, the cookie may be used to observe certain types of browsing behaviours, which are then combined with other browser data to give a picture of what people are likely to do when they surf the web.

How long are data stored?

The data obtained through ScorecardResearch cookies is kept for up to 90 days.

---

15 comScore. Fact Sheet (2013). *comScore is a leading internet technology company that provides Analytics for a Digital Worl*. Retrieved September, 16th, 2013 from: http://www.comscore.com/About_comScore/comScore_Fact_Sheet.

16 «Web beacons, also called web bugs and clear GIFs are used in combination with cookies to help people running websites to understand the behaviour of their customers. A web beacon is typically a transparent graphic image (usually 1 pixel x 1 pixel) that is placed on a site or in an email. The use of a web beacon allows the site to record the simple actions of the user opening the page that contains the beacon. […]Web beacons are typically used by a thir-party to monitor the activity of a site». Allaboutcookies.org. *Web Beacons and other Tools*. . Retrieved March, 4th, 2014 from: http://www.allaboutcookies.org/web-beacons/.

Are data sold to third parties?

According to comScore, the information collected through the web beacon is analyzed and the resulting reports are shared with their clients.

4. DISCUSSION

As stated in the controversial article published *Giving the Web a Memory Cost Its Users Privacy* published in The New York Times by John Schwartz[17], before the creation of cookies, «every visit to a site was like the first, with no automatic way to record that a visitor had dropped by before. Any commercial transaction would have to be handled from start to finish in one visit, and visitors would have to work their way through the same clicks again and again; it was like visiting a store where the shopkeeper had amnesia».

Cookies play an essential role in nowadays web development and are a useful tool to personalize content, helping users to customize their web navigation. These types of technologies can help web editors providing a better navigation experience to their visitors remembering i.e. users' preferred navigation language or font size, users' log-in data or making possible e-commerce services such as the shopping cart.

However cookies can be used as well to track users' behavior on the Internet with commercial purposes, such as web traffic measurement or personalized advertising.

Current Spanish legislation, after EU e-Privacy directive adoption, aims to make a more transparent Web. At the end, every Internet user has the right to known that his or her navigation generates valuable data to advertising companies. It is understandable websites collecting user's data (like, for instance, cybermedia) may have the obligation to clearly inform about the user's data they collect and the purposes those data will be used. It is, on the other hand, reasonable that users must give their consent to allow websites to collect their data. Most of cookies we have analyzed in this study are not strictly necessary to provide a communication service and, as a consequence, users should know they must be able to visit the same websites without being tracked.

There are some interesting initiatives in this field like the Do Not Track header which is trying since 2009 to standardize a technology could Internet users' allow web navigation without being tracked by third companies, although these kinds of projects have been unsuccessful to date.

17 Schwartz, J. (2001). Giving the Web a Memory Cost Its Users Privacy. *The New York Times*. Retrieved February, 14th, 2014 from http://www.nytimes.com/2001/09/04/technology/04COOK.html.

Maybe privacy is the price we have to pay for Internet free services like search engines, online media or social networks. As stated by Goodson[18] «If You're Not Paying For It, You Become The Product». Ramonet highlights in this sense the potential risks of a culture where information is becoming merchandise and social responsibility is subject to market requirements. In Ramonet's point of view[19], one of the most important risks we face in relation to digital information, is the three main functions of mass media (which sociologists have traditionally understood as inform, educate and entertain) can be become monitor, advertise and sell.

We can guess a future in increasingly interconnected and globalized societies. Maybe Internet user's data safety is one of the greatest challenges we will have to face in the coming years. In our opinion, a greater awareness in this field is required as well as a greater responsibility of the participants, in three different levels: institutions should have a duty to educate citizens about these issues, web editors and data collecting companies should better inform about their tracking methods and take initiatives to advocate for a greater transparency and finally, web users should understand the risks concerning their privacy they assume while surfing the Web and accept the consequences an irresponsible navigation may have for their data privacy.

5. BIBLIOGRAPHY

Agencia Española de Protección de Datos (AEPD) (2013). *Guía sobre el uso de las cookies*. Retrieved June, 5th, 2013 from http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf.

Article 29 Data Protection Working Party (2012). Opinion 04/2012 on Cookie Consent Exemption, Adopted on 7th June 2012. Retrieved June, 5th, 2013 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Article 29 Data Protection Working Party (2011), Opinion 15/2011 on The Definition of Consent. Adopted on 13th July 2013. Retrieved June, 5th, 2013 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf.

Barth, A. (2011) *HTTP State Management Mechanism*. Internet Engineering Task Force (IETF) Retrieved September, 5th, 2013 from <http://tools.ietf.org/pdf/rfc6265.pdf>.

18 Goodson, S. (2012) If You're Not Paying For It, You Become The Product. *Forbes*. Retrieved March, 10th, 2014 from: http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/.

19 Ramonet, I.(2002). Propagandas silenciosas. *En Arte y Literatura* (ed.) (p. 16-17), La Habana.

Boyd, D.; Ellison, N. (2007) *Social Network Sites: Definition, History, and Scholarship.* Journal of Computer-Mediated Communication. Retrieved July, 10th, 2013 from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf.

Castells, M. (2000) *Internet y la Sociedad en Red* .Conferencia de presentación del Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento. Universitat Oberta de Catalunya.

Castells, M. (2001) *La Galaxia Internet*. Ed: Areté (p. 43) Madrid.

Comscore. Fact Sheet (2013). *comScore is a leading internet technology company that provides Analytics for a Digital Worl*. Retrieved September, 16th, 2013 from: http://www.comscore.com/About_comScore/comScore_Fact_Sheet.

Cross, C.; Geary, J.; (2012) *Tracking the trackers: who are the companies monitoring us online?* Battle for Internet. The Guardian, 23th of April, 2012. Retrieved September, 16th, 2013 from: http://www.theguardian.com/technology/interactive/2012/apr/23/tracking-trackers-companies-following-online.

España. Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. *Boletín Oficial del Estado*, 12 de julio de 2002, núm. 166, pp. 25388-25403. Retrieved July, 10th, 2013 from: http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf.

España. *Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista*. *Boletín Oficial del Estado* , 31st of March 2012, 78, 26876- 26967. Retrieved September, 11th, 2013 from http://www.boe.es/boe/dias/2012/03/31/pdfs/BOE-A-2012-4442.pdf.

European Union (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Official Journal L 201 , 31st of July 2002, 0037-0047. Retrieved September, 11th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

European Union (2009). *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*. Retrieved September, 11th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

Fundación Orange (2013). *eEspaña 2013: informe anual sobre el desarrollo de la sociedad de la información en España.* Retrieved June, 5th, 2013 from http://www.proyectosfundacionorange.es/docs/eEspana_2013_web.pdf.

García-Ull, F.J. (2013): Las cookies en los principales cibermedios generalistas de España. *Miguel Hernández Communication Journal*, 4, 233-261.

Gomes, L. (1996) *Web 'Cookies' May be Spying on You*. San Jose Mecrury News.

Gómez, Rosario. (2013) *España adapta las cookies a Europa*. El País. Retrieved April, 29th, 2013 from: <http://tecnologia.elpais.com/tecnologia/2013/04/29/actualidad/1367260814_267849.html>.

Goodson, S. (2012) If You're Not Paying For It, You Become The Product. *Forbes*. Retrieved March, 10th, 2014 from: http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/.

Hodges, Dept. of Comput. Sci., Univ. of Oxford, Oxford, UK D.; Creese, S. (2013). Breaking the Arc: Risk control for Big Data. *IEEE Big Data 2013*, 613-621.

Information Commisioner's Office (ICO) (2012) *Guidance on the rules on use of cookies and similar Technologies*. Privacy and Electronic Communications Regulations. Retrieved September, 11th, 2013 fromhttp://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.

International Conference of Data Protection and Privacy Commissioners, Madrid, (2009). Retrieved July, 10th, 2013 http://www.privacyconference2011.org/htmls/adoptedresolutions/2009_Madrid/2009_m1.pdf.

Jackson, T. (1996) *This Bug in Your PC is a Smart Cookie*. Financial Times.

Lessig, L. (2006) «*CODE v.2.0*» Basic Books, New York.

Martínez, E.; Muñoz, M. (2013) *En busca de equilibro entre la regulación y la autorregulación de la publicidad comportamental en línea*. Estudios sobre el Mensaje Periodístico. Vol. 19. Servicio de Publicaciones de la Universidad Complutense, Madrid.

Montulli, L. (2000) *RFC 2965 HTTP State Management Mechanism* Network Working Group. IETF. Netscape Communication, Retrieved September, 9th 2013 from: http://tools.ietf.org/html/rfc2965.

Montulli, L. (1997) *RFC 2109 HTTP State Management Mechanism* Network Working Group. IETF. Netscape Communications, Retrieved September, 9th 2013 from: http://tools.ietf.org/html/rfc2109.

Ramonet, I.(2002). Propagandas silenciosas. *En Arte y Literatura* (ed.) (p. 16-17), La Habana.

Schwartz, J. (2001). Giving the Web a Memory Cost Its Users Privacy. *The New York Times*. Retrieved February, 14th, 2014 from http://www.nytimes.com/2001/09/04/technology/04COOK.html.

DEVELOPMENTS ON DATA PROTECTION IN BRAZILIAN LAW

Leonardo Mattietto
Professor de Direito Civil na Universidade Federal do Estado do Rio de Janeiro,
Procurador do Estado do Rio de Janeiro

ABSTRACT: In spite of its more than 200 million inhabitants and of being among the world's largest economies, Brazil does not yet have a comprehensive legislation regarding personal data protection. As the Constitution and the Civil Code ensure privacy –at least in the sense of the right to private life–, and the Consumer Protection Code generically protects consumers data, the judicial courts have emanated numerous decisions on cases of breaches of personal data, but the Brazilian law remains far from the global context. There is neither agency nor public authority in charge of the protection of personal data.

However, there were approved the law that regulates access to public information (2011) and the cybercrime statute (2012).

The National Congress recently passed the so much expected Marco Civil of the Internet (2014), which results from a democratic and legitimate process. This new law sets forth the principle of net neutrality and enhances privacy, as well as requires express consent for the collection and transfer of personal data, and establishes penalties and compensation for damages. The government has backed down from the controversial requirement that companies would have to store data on servers physically located in Brazil.

Moreover, the Ministry of Justice has prepared a draft of a bill on the protection of personal data, which will create the National Council for the Protection of Personal Data. It is expected to be sent to the Congress soon.

KEYWORDS: Privacy; data protection; personal data; Marco Civil; internet in Brazilian law.

1. A BRIEF HISTORY AND CONTEXT OF DATA PROTECTION IN BRAZIL

Brazil does not yet have a comprehensive data privacy law[1], but its main principles are all set by the Constitution of the Republic (1988). These principles, taken together,

1 It is possible to say that «Brazilian law does have a *privacy framework*, although it is not comprehensive». Costa, Luiz. *A Brief Analysis of Data Protection Law in Brazil*, p. 16. Retrieved December 20th, 2013, from http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf.

build a viable system of privacy protection, by declaring the right to privacy inviolable and guaranteeing compensation to everyone who suffers damages.

As fundamental human rights, Article 5 of the Constitution proclaims that «the expression of thought is free, and anonymity is forbidden» (item IV); «the intimacy, private life, honor and image of people are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured» (item X); «the home is the holy and inviolable refuge of the individual, and no one may enter therein without the consent of the dweller, except in the event of flagrant delict or disaster, or to give help, or, during the day, by Court order» (item XI); «the secrecy of mail and of telegraphic data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts» (item XII), and «*habeas data* shall be granted to ensure the access to the knowledge of information related to the person of the petitioner, contained in records or data banks of government agencies or of agencies of a public character or for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative» (item LXXII).

The Consumer Protection Code (1990) protects consumer data in databases and files and lays out procedures for record keeping, plus guidelines for informing data subjects. But, unlike the role the Federal Trade Commission performs in the United States for privacy, Brazil has no personal data bureaucracy. The so called «Procons», agencies in charge of the consumers' protection, created more than 20 years ago to enforce consumer law, have not chosen to safeguard personal data among their priorities and have been more dedicated –successfully– to ensure economic interests of the consumers.

The Civil Code (2002) does not even mention personal data, but states that «the private life of a natural person is inviolable, and the judge, on application by the interested party, shall adopt such measures as may be necessary to prevent or cause to cease any act contrary to this provision» (Article 21). All violations should be considered illicit acts (Article 186) and «anyone who, through an illicit act causes damage to another is obligated to repair it» (Article 927). It is known that «the combined application of the above mentioned rules implies thus that the alleged victim of a privacy violation can ask the court to adopt substantive measure aimed to prevent and, more realistically, to terminate such violation and to assign compensation»[2].

The Access to Public Information Act (Federal Law nr. 12.257, of 2011) defines that personal data stored by the State will have restricted access, regardless of classification of secrecy, for a maximum of one hundred years from the date of its production.

2 Parrilli, Davide M.; De Conti, Rafael. *Data Protection Law in Brazil: an overview*. Retrieved December 20th, 2013, from http://www.decontilaw.com/Artigos/Data%20Protection%20Law%20in%20Brazil_DMP_100312_RDC_110312_forDCLO.pdf.

Anyway, it does not clarify what is personal data and its enforceability depends on future provisions by law. Therefore, «despite this 100-year duration, which can seem that privacy is protected, there is no legal criterion to balance conflicts between the rights to privacy and the citizen's right to information, which can lead to the total absence of guidelines and ultimately to conflicts»[3].

In the same year, the Brazilian Congress passed the Credit Information Act (Federal Law nr. 12.414, of 2011), which promotes, with fairly poor results until now, «the creation and the access to databases related to credit information of citizens and companies».

In 2012, there were approved two laws on cybercrime (Federal Laws nrs. 12.735 and 12.737). The National Congress reacted after the famous actress Carolina Dieckmann had nude photos stolen from her computer by a technician and largely published on the web. These laws criminalize hacking and unauthorized access of information technology, with higher penalties for breaching data of public officials. It has become a crime to interrupt phone or internet services, and to falsify credit cards. Police should create specialized units to investigate cybercrimes.

Angered by the disclosure of the systematic and massive electronic surveillance and interception by the United States, after the National Security Agency espionage scandal, Brazil and Germany presented a resolution to the United Nations urging countries to extend privacy rights to all individuals and calling for an end to unlawful and arbitrary violations. This resolution was adopted by the General Assembly of the United Nations on December 18th, 2013, reaffirming the human right to privacy, by a text entitled «Right to privacy in the digital age».

In this historical context, it is important to notice that «in Brazil, the concept of privacy and the instruments for its protection have undergone constant development in recent years by both courts and legislatures, to deal with the challenges of data processing. Although Brazil does not have a general data protection law as do several South American countries, a data protection framework is being developed from various elements such as the privacy rights provided in the Brazilian Constitution or several statutes that deal directly with personal data»[4].

Thus, in relation to the constitutional right to privacy (or the universal fundamental right to privacy which starts to be modeled by Public International Law), data

3 Costa, Luiz. *A Brief Analysis of Data Protection Law in Brazil*, p. 8. Retrieved December 20th, 2013, from http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf.

4 Doneda, Danilo; Mendes, Laura Schertel (2014). Data Protection in Brazil: new developments and current challenges. In S. Gutwirth, R. Leenes, P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (p. 4). Dordrecht: Springer.

protection is increasingly becoming a matter of autonomous regulation in Brazil, what can be seen as a turning point in this matter[5].

2. MARCO CIVIL OF THE INTERNET

2.1. Law-making process and legitimacy

The Marco Civil (Civil Rights Framework for the Internet) started as an initiative from the Ministry of Justice, in partnership with the Center for Technology and Society of Fundação Getúlio Vargas School of Law. There was developed a collaborative and multistakeholder process in which both the government and civil society could work to define the principles and rules that should guide the use of the internet in Brazil. The result was a bill of law (nr. 2.126) which was submitted to the National Congress in August 2011.

The draft bill was officially named Marco Civil (the word «civil» as opposed to a criminal framework), placing internet access as an essential right to citizenship. The online consultation was divided into two periods, each of them of about 45 days.

In the first period of the consultation, there was «a debate about general principles, which then served as reference for the writing of the text of draft bill. These principles were divided into three groups: (1) individual and collective rights (privacy, freedom of speech, and access rights), (2) principles related to intermediaries (net neutrality and civil liability), and (3) governmental directives (openness, infrastructure, and capacity building)»[6].

The draft text for the bill, reflecting the comments received on its first phase, was then put under consultation for the second period, when «contributions were received through a website hosted by *Cultura Digital*, an online platform developed by the Ministry of Culture, with the goal to encourage the emergence of online communities for the discussion of public policies for the digital environment. During both periods of the consultation, users were allowed to comment on the consultation texts, paragraph by paragraph, directly in the website. Nonetheless, blog posts, tweets, articles published in mainstream media, and institutional and individual contributions sent by email (and then made available to the public at the website) were also taken into consideration»[7].

---

5 Doneda, Danilo; Mendes, Laura Schertel (2014). Data Protection in Brazil: new developments and current challenges. In S. Gutwirth, R. Leenes, P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (p. 4). Dordrecht: Springer.

6 Fundação Getúlio Vargas. *Civil Rights Framework for Internet in Brazil*. Retrieved December 22nd, 2013, from http://direitorio.fgv.br/civilrightsframeworkforinternet.

7 Fundação Getúlio Vargas. *Civil Rights Framework for Internet in Brazil*. Retrieved December 22nd, 2013, from http://direitorio.fgv.br/civilrightsframeworkforinternet.

The draft sent by the government to the National Congress established principles, guarantees, rights and obligations concerning the use of the Internet (Articles 1 to 6), by securing basic rights and guarantees to users (Articles 7 and 8), regulating internet connection and applications (Articles 9 to 18), defining the role of public authorities (Articles 19 to 23) and promoting the protection of interests that can be exercised in court, individually and collectively (Articles 24 and 25).

It can be noticed that «the very idea of Marco Civil was a radical change in the perspective on how law and politics could be conducted by a government. The Marco Civil is (…) a law proposition, formulated in great part outside the legislative houses of the Brazilian Congress. The idea was to obtain the draft of the bill from the society prior the necessary step of sending it to be voted and negotiated by the congressmen, and the radical concept was to use the internet itself to formulate a law meant to regulate the internet; in an extreme democratic approach the debate would be opened to everyone, including non-nationals of Brazil»[8].

The participation of many groups with conflicting interests and the openness and transparency of the process have helped to improve the legitimacy of the bill[9]. However, the legislative process of the Marco Civil was delayed over concerns about how the law should regulate internet. After the PRISM electronic surveillance was unveiled, the government prioritized the bill, which was charged with constitutional urgency in September 2013, as a reaction to allegations made by Edward Snowden on spying against the Brazilian government, citizens and companies.

---

8 Souza Filho, Rubens A. Menezes de. *The struggle over privacy, security, cyber-crimes and the civil rights in the Brazilian law – a historical overview*, p. 12. Retrived December 20th, 2013, from http://geptec.fflch.usp.br/sites/geptec.fflch.usp.br/files/Rubens%20Menezes%20-%20The-Struggle-over-Privacy-Security-Cyber-Crimes-and-the-Civil-Rights-in-the-Brazilian-Law-a-Historical-Overview.pdf.

9 «Predictably, debates that involved the balance between conflicting rights and interests, freedom of speech, anonymity, privacy and access rights were the topics of heated and often rich debates during both stages of the consultation process. Over 2,000 contributions, from individual users, governmental and non-governmental entities were received. NGOs, universities, internet service providers (collectively through associations, as well as individually), business companies, law firms, law enforcement agencies, individuals, Brazilian Embassies from all over the world, and many other participants have joined the online public hearing. The participation of several stakeholder groups has promoted the diversity of opinions and the availability of high quality information and expert advice, which have helped the government to draft a balanced bill. The openness and transparency of the process, entirely conducted online, in the public eye, has improved the legitimacy of the bill. Marco Civil was introduced in Congress with the political weight and the legitimacy that the bill would be expected to have after a complex multistakeholder discussion». Fundação Getúlio Vargas. *Civil Rights Framework for Internet in Brazil*. Retrieved December 22nd, 2013, from http://direitorio.fgv.br/civilrightsframeworkforinternet.

In February 2014, a brand-new version of the bill was introduced by Rapporteur Alessandro Molon, Congressman of the Labour Party from Rio de Janeiro, by request of President Dilma Rousseff. From this version, some points shall be highlighted.

The Rapporteur included that regulation of internet in Brazil should be based on safeguarding freedom of expression and should have, among its pillars, the development of the personality and the network's social purposes (Article 2).

The inviolability of intimacy and privacy was declared by Article 7 and its protection was guaranteed, as well as compensation for material or moral damages resulting from violation. The same article brought the «inviolability and secrecy of private communications stored, except by court order» and connection logs and access records were expressly considered personal data, which should not be shared with third parties.

Moreover, Article 7 has set the right «to clear and complete information on the collection, use, storage, processing and protection of personal data, which can only be used for purposes which: a) justify its collection; b) are not prohibited by law; and c) are specified in contracts for services», the right to express consent, «which should occur prominently based upon the other contractual clauses», the right «to the definitive exclusion of personal data provided to the internet application, if asked by the user, at the end of relationship between the parties» and to the publicity and clarity of existent connection providers and internet application providers policies.

Article 8 provided that should be null and void the contract terms that violate the right to privacy, specially those that offend the inviolability and secrecy of communications and, in adhesion contracts, do not offer an alternative to resort the Brazilian courts for resolving disputes arising from services rendered in Brazil.

Article 10 stated the content of private communications should be available only by court order, in the cases and in the manner provided by law.

Article 11 declared that «any process of collection, storage, custody and treatment of records, personal data or communications by connection providers and internet application providers, in which at least one of these acts occurs in the national territory, shall respect Brazilian law».

On the version presented by the Rapporteur, Article 12 would entitle the government to require data storage in Brazil. This point did not pass on the final text voted by the Congress, but, as one of the main cores of the government reaction to espionage –somewhat like a magic act to solve such a complex international problem–, this will be discussed later on this paper.

On March 25th, 2014, the bill was finally approved by the House of Representatives and submitted to the Senate, after long and intense political negotiation, riddled with some distrust and even bad faith, and overcoming several failed attempts of having it voted.

The bill was processed unusually fast by the Senate, being unanimously accepted within less than a month, on April 22nd, 2014. President Rousseff sanctioned the law

at the opening ceremony of *NETmundial*, a world conference held in São Paulo which main goal was to discuss the future of internet governance.

The Marco Civil, now Federal Law nr. 12.965, will become effective sixty days after its official publication held on April 24th, 2014, when it will be mandatory to public and private entities, as well as to individuals. Its principles and rules will be fully enforceable by government officials and by the courts.

The approval of the Marco Civil means a glaring advance for legal security in Brazilian cyberspace, «filling Brazil's regulatory gaps, which currently thwart investment in its technology infrastructure, such as the lost opportunity with Google's data center wherein Chile was victorious»[10]. Upon the enactment of the Marco Civil, Brazilian government hopes to lead the effort in internet governance, reducing exposure to litigation[11] and providing a bill of rights to users and safety to companies.

2.2. Net neutrality

The principle of network neutrality, set by the Marco Civil, has been in the eye of the storm of the political debate in the House of Representatives of Brazilian Congress. Article 9 of the Marco Civil ensures that «the agent in charge of transmission, switching and routing is obliged to treat any data packets with isonomy, regardless of content, origin and destination, service, terminal or application». Providers of internet connection are forbidden to block, monitor, filter, analyze or inspect the content of data packets. Services should be performed on a non-discriminatory way and refrained from anticompetitive practices.

Telephone companies wanted to overthrow the principle of net neutrality, that guarantees equality to all information, so that they could sell packets with different contents and prices, as on cable. The leader of the second major Party in the Brazilian Congress, which has been president of a telecom company in the past, used his strong influence as party leader to convince other Congressmen to prevent the network remained neutral, so that these corporations could choose which content would be free and which would have to be paid to go on the net. His attitude posed a risk not only for the internet as we know it today, but for all civil, social and political rights.

---

10 Fortes, Vinicius B. *Privacy protection in cyberspace: the Brazilian case*, p. 13. Retrieved February 20th, 2014, from http://cglad.com.br/wp-content/uploads/2013/06/1.-ViniciusBorgesFortes_PrivacyCyberspace_Final_2013.pdf.

11 Brazil has been one the leading countries in takedown requests and lawsuits against Google. For instance, from July to December 2012, Google has received 640 requests from Brazilian courts or prosecutors to remove contents, while there were 262 from the United States in the same period. See http://www.google.com/transparencyreport/removals/government/countries/?p=2012-12.

Tainted by commercial purposes, as companies pushed for continue to base their business on data discrimination, Article 9 of the Marco Civil has become one of the main fields of political battle at the Brazilian Congress. On the other hand, some Congressmen believed that internet should not suffer any kind of government intervention.

Nevertheless, network neutrality is the principle that enshrines that internet users should be able to access any web content they choose and use any applications they want, without any restrictions imposed by their internet service provider. For instance, if someone is shopping online for a new appliance, he should be able to shop on any websites, not just the ones with whom his provider has a preferred business relationship. Internet providers should not be able to block content for commercial purposes as, for example, to make phone calls using a high-speed connection.

Accordingly to the principle of net neutrality, the government also should not control which websites can and cannot be accessed, as unfortunately happens in undemocratic countries. It is important to keep internet free and open to everybody.

2.3. Data storage on servers located in Brazil

On the version presented by the Rapporteur in February 2014, Article 12 of the bill affirmed that «the Executive Branch, through Decree, may force connection providers and internet application providers who exercise their activities in an organized, professional and economic way, to install or use structures for storage, management and dissemination of data in the country, considering the size of the providers, its sales in Brazil and breadth of the service offering to the Brazilian public». The violation could lead to a fine of up to ten percent of the gross revenues of the economic group in Brazil in its last financial year and temporary suspension or even the prohibition of its activities.

This measure could be technically difficult to put into practice, very expensive and also hard to enforce[12]. Regrettably, storing data in-country as an extremely protectionist

12 «Governments implementing in-country data mandates imagine that the various global services used in their country will now build infrastructure locally. Many services, however, will find it uneconomical and even too risky to establish local servers in certain territories. Data centers are expensive, all the more so if they have the highest levels of security. One study finds Brazil to be the most expensive country in the Western hemisphere in which to build data centers. Building a data center in Brazil costs $60.9 million on average, while building one in Chile and the United States costs $51.2 million and $43 million, respectively. Operating such a data center remains expensive because of enormous energy and other expenses – averaging $950,000 in Brazil, $710,000 in Chile, and $510,000 in the United States each month. This cost discrepancy is mostly due to high electricity costs and heavy import taxes on the equipment needed for the center. Data centers employ few workers, with energy making up three-quarters of the costs of operations. According to the 2013 Data Centre Risk Index –a study of thirty countries on the risks affecting successful data center operations– Australia, Russia, China, Indonesia, India, and

measure is the internet dream of totalitarian countries. Anyway, Brazil is a market too big to be despised by international internet corporations.

Data storage in Brazil would not seem to enhance either privacy or security of Brazilians and could bring the risk of breaking apart the web[13].

Furthermore, such data storage requirements could threaten the major new advances in information technology. It is relevant to say that «data localization requirements also interfere with the most important trends in computing today. They limit access to the disruptive technologies of the future, such as cloud computing, the Internet of Things, and data driven innovations (especially those relying on big data). Data localization sacrifices the innovations made possible by building on top of global internet platforms based on cloud computing. This is particularly important for entrepreneurs operating in emerging economies that might lack the infrastructure already developed elsewhere. And it places great impediments to the development of both the Internet of Things and big data analytics, requiring costly separation of data by political boundaries and often denying the possibility of aggregating data across borders»[14].

After big political pressure and lobbying, the government has given up on local data storage, in order to get the necessary support to pass the bill.

Although the government has backed down from its intentions to demand that companies store data locally, the law still requires that companies will be subject to Brazilian rules in case of legal disputes involving data, regardless of whether it is stored.

3. BILL OF LAW ON PERSONAL DATA PROTECTION

A personal data protection bill has also been developed by the Ministry of Justice in Brazil and it is expected to be sent to the National Congress soon. Although this bill can

---

Brazil are the riskiest countries for running data centers». Chandler, Anupam; Lê, Uyên P. *Breaking the Web: Data Localization vs. the Global Internet*, pp. 36-37. Retrieved March 12th, 2014, from http://ssrn.com/abstract=2407858. Amounts are expressed in US Dollars.

13 «Data localization requirements threaten the major new advances in information technology – not only cloud computing, but also the promise of big data and the Internet of Things. Equally important, data localization requirements undermine social, economic and civil rights by eroding the ability of consumers and businesses to benefit from access to both knowledge and international markets and by giving governments greater control over local information. Legitimate global anxieties over surveillance and security are justifying governmental measures that break apart the World Wide Web, without enhancing either privacy or security». Chandler, Anupam; Lê, Uyên P. *Breaking the Web: Data Localization vs. the Global Internet*, p. 1. Retrieved March 12th, 2014, from http://ssrn.com/abstract=2407858.

14 Chandler, Anupam; Lê, Uyên P. *Breaking the Web: Data Localization vs. the Global Internet*, p. 40. Retrieved March 12th, 2014, from http://ssrn.com/abstract=2407858.

be considered very similar to the European Union Data Protection Directive nr. 95/46/EC, it is necessary to see that «Brazil's choice, however, is not yet done. It is expected that the respect for human dignity, enshrined by the Constitution, as well as the civilian tradition that our system reflects, coupled with globalization through civil rights, allow the approach to the European model, favoring legislation by principles»[15]. It is also helpful to remark that the Council of Europe Convention nr. 108 and its modernization proposals[16] have had a strong influence on this text.

The draft sets forth general provisions (Articles 1 to 8), proclaims the principles of data protection –finality, necessity, free access, proportionality, data quality, transparency, security, good faith, responsibility and prevention (Article 8), a consent framework (Articles 9 to 13), rights of data subjects, as access, rectification and erasure (Articles 15 to 19), protection to sensitive data (Articles 20 to 22), data security (Articles 23 to 27), data processing rules for governmental and private databases (Articles 28 to 34), transborder[17] data flow rules (Articles 35 to 37), supervisory authority and enforcement (Articles 38 to 44), best practice codes (Article 45) and final provisions (Articles 46 to 48).

As the approval of this bill seems so far away to appear on the horizon, personal data protection in Brazil shall rely on the principles enshrined by the constitutional system and stand side by side with the rights of personality, being considered a corollary of the general right to privacy provided by the Article 21 of the Civil Code. It is useful to think that «a so much hatched weft of principles for the protection of personal data responds to the reality of a matter which, in its breadth and for its tendency to application in every kind of human relationship, cannot be entrusted solely to casuistic rules. Legislation by principles, so that it can achieve its purposes, should serve to define a general framework within which specific provisions should be made and interpreted later»[18].

---

15 Moraes, Maria Celina Bodin de (2008). Apresentação. In Stefano Rodotà, *A vida na sociedade de vigilância: a privacidade hoje* (p. 12). Rio de Janeiro: Renovar.

16 «The 'globalisation' of Convention 108 (developing it into a global data privacy agreement, open to all countries providing the required level of data protection) is also now underway, and Uruguay has become the first non-European state to become a Party to the Convention. The advantages of 'globalisation' are significant for both existing parties and new entrants, but these advantages depend upon the Convention requiring a sufficiently high level of privacy protection for non-European accessions (including restrictions on data exports to recipients in states not parties to the convention), and requiring that these protections continue to be provided in practice». Greenleaf, Graham. *'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?*, p. 2. Retrieved April 20th, 2014, from http://ssrn.com/abstract=2262296.

17 The bill inserts an European Union-style adequacy standard that would prohibit data transfers outside of Brazil unless the recipient country ensures an adequate level of data protection.

18 Moraes, Maria Celina Bodin de (2008). Apresentação. In Stefano Rodotà, *A vida na sociedade de vigilância: a privacidade hoje* (p. 11). Rio de Janeiro: Renovar.

The future Personal Data Protection Act will also create the National Council for the Protection of Personal Data (Article 38) as the authority in charge of enforcing the legislation. The performance of such an authority, «although strange to the current landscape of the matter in Brazil, deserves attention and detained account. Firstly, because in this case the mere action of the individuals to protect their interests –individual control, such as occurs in some of the conceptions of protection of personal data (…)– is not able to design a situation in which the concerned fundamental right receives appropriate protection and ultimately reflects a particular ideological view of the interests at issue, mitigated by an apparent concession of power to the individuals, does not entail the effective protection of their interests»[19].

The creation of an independent authority for the protection of personal data, better than the protection by judicial courts in response to individual actions, means the fulfillment of an institutional guarantee, as there is the severe risk that the Judiciary Branch may produce conflicting and contradictory decisions on issues that are directly related to the use of the internet[20]. The profusion of decisions emanated from the several state courts have shaped a chaotic and incoherent system, where privacy is not adequately protected and big mistakes are possible due to the lack of secure rules. The regulation by law and its enforceability by a single national authority could replace the current inconsistent patchwork.

It must be recognized that «the impossibility of an informational self-determination based on the unique action of the individual is evident in view of the disparity between his will and the existence of structures for data collection prepared to exclude him from certain advantages if he decides not to provide it – thus, that individual protection reproduces a rather elitist tradition of privacy, not corresponding to the current position in our Constitution nor to other rights that must be measured in this situation, such as equality»[21].

4. CONCLUSIONS

The Marco Civil is the result of a long-running consensus-building process. Net neutrality is a good provision not only to prevent undemocratic and undue governmen-

19 Doneda, Danilo (2006). *Da privacidade à proteção de dados pessoais* (p. 399). Rio de Janeiro: Renovar.

20 Fortes, Vinicius B. *Privacy protection in cyberspace: the Brazilian case*, p. 13. Retrieved February 20th, 2014, from http://cglad.com.br/wp-content/uploads/2013/06/1.-ViniciusBorgesFortes_PrivacyCyberspace_Final_2013.pdf.

21 Doneda, Danilo (2006). *Da privacidade à proteção de dados pessoais* (pp. 399-400). Rio de Janeiro: Renovar.

tal intervention, but a valuable principle to protect equality and the right of internet users to access any web content they choose, without any restrictions imposed by their internet service provider.

Local data storage, intended by the Brazilian government, was a protectionist political decision that could turn out to be highly ineffective. A better and safer internet should not require breaking it apart. Fortunately, it was not approved by the National Congress.

The creation of an independent authority to protect personal data would be a more intelligent measure than the storage of data only in data centers located in the Brazilian territory. The foundation of the National Council for the Protection of Personal Data is not only necessary, but indispensable to enforce privacy rights over the internet.

5. BIBLIOGRAPHY

Chandler, Anupam; Lê, Uyên P. *Breaking the Web: Data Localization vs. the Global Internet*. Retrieved March 12th, 2014, from http://ssrn.com/abstract=2407858.

Costa, Luiz. *A Brief Analysis of Data Protection Law in Brazil.* Retrieved December 20th, 2013, from http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf.

Doneda, Danilo (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.

Doneda, Danilo; Mendes, Laura Schertel (2014). Data Protection in Brazil: new developments and current challenges. In S. Gutwirth, R. Leenes, P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (pp. 3-20). Dordrecht: Springer.

Greenleaf, Graham. *'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?* Retrieved April 20th, 2014, from http://ssrn.com/abstract=2262296.

Moraes, Maria Celina Bodin de (2008). Apresentação. In Stefano Rodotà, *A vida na sociedade de vigilância: a privacidade hoje* (pp. 1-12). Rio de Janeiro: Renovar.

Fortes, Vinicius B. *Privacy protection in cyberspace: the Brazilian case*. Retrieved February 20th, 2014, from http://cglad.com.br/wp-content/uploads/2013/06/1.-ViniciusBorgesFortes_PrivacyCyberspace_Final_2013.pdf.

Fundação Getúlio Vargas. *Civil Rights Framework for Internet in Brazil*. Retrieved December 22nd, 2013, from http://direitorio.fgv.br/civilrightsframeworkforinternet.

Parrilli, Davide M.; De Conti, Rafael. *Data Protection Law in Brazil: an overview*. Retrieved December 20th, 2013, from http://www.decontilaw.com/Artigos/

Data%20Protection%20Law%20in%20Brazil_DMP_100312_RDC_110312_forDCLO.pdf.

Souza Filho, Rubens A. Menezes de. *The struggle over privacy, security, cyber-crimes and the civil rights in the Brazilian law – a historical overview.* Retrived December 20th, 2013, from http://geptec.fflch.usp.br/sites/geptec.fflch.usp.br/files/Rubens%20Menezes%20-%20The-Struggle-over-Privacy-Security-Cyber-Crimes-and-the-Civil-Rights-in-the-Brazilian-Law-a-Historical-Overview.pdf.

DATA PROTECTION MANAGEMENT SYSTEM A FUTURE ORGANIZATIONAL APPROACH TO HANDLE GROWING QUANTITIES OF DATA?

Philipp E. Fischer
Ph.D. cand., Internet Interdisciplinary Institute (IN3), UOC Barcelona
LL.M. in Intellectual Property Law (London/Dresden)
Chief Compliance- & Privacy Officer, SuiGenerisData GmbH, Munich

Ricardo Morte Ferrer
Lawyer (Abogado)
Master in Information and Knowledge Society (UOC)
Data Protection Advisor, SuiGenerisData GmbH, Munich

ABSTRACT: Over the past years, the European Parliament and the Council have been constantly working on the harmonization of the legal framework for the protection of personal data in the EU. They have now proposed a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

Within the validity of the current data protection legislation and the proposed General Data Protection Regulation, an organization which processes personal data, has to give proof that its business processes do not affect people´s personal data in an unacceptable way. To furnish proof of this will be increasingly difficult because of the ever-increasing amount whilst collection, processing and use of personal data in the future economy. This is especially true for large or structurally very diverse organizations or those who process a large number of objective data (Big Data).

The future level of data protection in such cases will therefore increasingly depend on a more structural approach. To solve this problem, this contribution suggests the setting up of a data protection management system (DPMS). A DPMS essentially supports the work of a data protection officer and intends to enable an organization to exercise a systematic planning, monitoring, intervention and support function of their own data protection compliance in a standardized and as much as possible automatized way.

KEYWORDS: Privacy, Data Protection Management System, Information Security Management System, Standard Datenschutz Modell, ITIL®, COBIT®.

1. INTRODUCTION

1.1. General Data Protection Regulation (GDPR) draft

In the age of Facebook, Google and smartphones, a data protection reform is urgently needed, which also stated the Austrian MEP Josef Weidenholzer (SPÖ). «The right to delete your own data and also to accurately control what data can be transmitted to private companies, is, not only since the NSA scandal, becoming increasingly important.»[1]

In January 2012 the European Commission presented its proposal for a new data protection regulation in Europe. The new regulation has the potential to successfully modernize data protection in Europe by adapting legislation to the challenges of technological and social developments.

The European Parliament approved on Wednesday 12 March 2014 a draft version of the GDPR, which provides stricter penalties for violations and a better protection of privacy. The plenary session in Strasbourg gave 621 votes in favor, 10 votes against and 22 abstentions. The new rules will on the one hand improve the protection of personal data and on the other hand facilitate data traffic within the EU.

The GDPR provides strict penalties for companies of up to five percent of annual sales or up to 100 million euros for data breaches. Citizens have the right to delete personal data and to allow the use of their data only by explicit permission. Companies need to explain in a clear and simple language to what extend the data are used.

However, in our opinion, the proposal in its current form is no more than a patchwork of good ideas. It lacks a coherent, all-encompassing approach that ensures by clear enforceable standards that, on the one hand, to have the fundamental rights of EU citizens respected, and on the other hand that innovative business models continue to be developed.

1.2. Effectiveness between data protection and corporate processes

Information is the most important asset in companies across the world. Anything that threatens the information as the basis of IT structure directly puts the whole company's performance at risk: e.g. confidentiality, accuracy, or currency of the information or its processing functions. The early involvement of IT governance and appropriate structuring of IT processes is necessary both from an economic and a security perspective. Conversely, IT security can only be implemented effectively if all safety measures relate to clearly defined processes and service requirements. The synergy between the law and the technique should optimize processes according to these premises.

One key example is the importance of the handling of Big Data. Data is a new form of value. In the digital world, it appears as the fourth factor of production in addi-

1 Weidenholzer (2014).

tion to capital, labor and raw materials. Therefore, data is sometimes named as the «oil of the future».» The value is not the data itself, but the insights that can be derived from the predominantly unstructured data through a new method. This scientific discipline is called «analytics». Its global sales in 2012 amounted to about 4.6 billion euros, as a calculation of the Experton Group[2] showed. The growth of this market segment will reach more than 30 percent - annually. Companies that process large amounts of data, such as banks or insurance companies, rank IT assets now at the «core of their business».» Big Data technologies play an important role in such departments wherever qualitatively different data is being collected in high volumes; so in research and development, production, distribution and logistics, finance and risk control as well as in marketing and sales.

1.3. Possible solution: Data Protection Management System (DPMS)

Within the validity of data protection law and its constitutional- and European law foundations, any company which processes personal data must be able to demonstrate that its business processes do not affect people in a constitutionally unacceptable way. Thus, an increasing quantity of corporate processes depends, at every step of the information life cycle, on the handling of personal data. The aim should be easily support companies manage data appropriately at every step of the information life cycle.

To achieve this, we need a concept for strong, coherent and effective concept. At the same time, this concept needs to create incentives for companies to invest throughout the whole life cycle on the protection of personal data, starting with the collection and processing of personal data.

The concept of a DPMS could help at this point. A DPMS is based on a simple principle: Those who invest from the beginning in a sustainable DPMS and ensure that they keep the conditions of the mechanisms within this DPMS, will be able to benefit from the advantages of an effective implementation and enforcement architecture.

2. SUPPORTIVE AND OPPOSING RELATIONSHIP BETWEEN DPMS AND ISMS

A DPMS has to put an organization in a position to exercise a systematic planning, monitoring and support function on its own data protection compliance- and in a standardized and machine-based way. A DPMS describes a type of requirements which an Information Security Management System (ISMS) does not know. An ISMS directly protects an organization´s own interests and assets. A DPMS has, however, an additional point of view from the outset by taking into account the interests of third parties.

2 Gerick, T. (2012).

A DPMS is firstly to meet the transparency requirements of organizations. It has to actively support the information needs of persons outside of these organizations, auditing activities of internal auditors and external supervisory authorities. In addition, a DPMS should maintain techniques that help affected persons to manage their data within organizations. And it should support infrastructures that conserve the purpose of a data processing. This aspect includes for example infrastructures that were developed as part of the (user-controlled) identity management. These techniques and infrastructures put organizations in a position to deal with secure identity attributes as well as with role pseudonyms or anonymous credentials. Last but not least a DPMS should initiate the evaluation of data protection procedures and track this progress.

An ISMS defines the systematic approach to legal requirements, such as those of data protection law, only insofar as the risks of non-compliant violations are assessed from the perspective of business processes. An ISMS takes not qua infrastructure side for the rights of those affected. DPMS and ISMS are in this respect both in a mutually supportive and opposing relationship when it comes to the implementation of requirements for the processing of personal data and this difference should be stressed in the present discussion.

3. DIFFERENT APPROACHES TO A DPMS

3.1. Priventum Initiative

The Priventum Initiative has been developed by Datenschutz Cert GmbH. It targets the establishment of a DPMS and aims at a high level of compliance with data protection legislation. It would allow organizations having this DPMS properly implemented to obtain a certificate as a guarantee of this compliance level.[3]

Priventum criteria follow more or less the PDCA cycle, as happens in the ISO Standards 27001 and 9000. This could be an advantage, allowing the integration of the DPMS within other processes which are applying these ISO Standards. In the following points we will shortly research the different phases of the PDCA cycle in the Priventum model for a DPMS:

- PLAN: Appointment of a DPO and implementation of the necessary structures for high data protection level, for example an adequate appointment of a DPO, a person with adequate knowledge, legal and IT, knowledge. The DPO should be integrated in all relevant processes in the organization. Research and document the status quo of data protection level in the organization. Analysis of the structures and possible risks. Following the points mentioned, the organization should work out a list including data protection requirements.

3 Maseberg (2012).

- DO: Implementation of the results about process management, IT security and data protection concept of the plan stage.
- CHECK: The DPO should control all the processes and audit the organization continually, in order to achieve legal compliance with the Data Protection legislation, according to § 4g Abs. Nr. 1 BDSG and including the technical and organization measures included in § 9 BDSG.
- ACT: All the problems found in the Check Phase must be resolved and this changes must be included in the documents

Which are the advantages of a DPMS? The implementation of a DPMS improves the synergy of processes in the organization, determines standards that could be demonstrated to customers and other stakeholders. This is the biggest achievement of Priventum. From our point of view, a weakness from Priventum consists in mixing ISMS and DPMS without giving detailed explanations. This could affect the implementation phase when it comes to different issues with different targets, which possibly could be developed in coordination but in separated ways.

3.2. ISO 27001

This is a Standard for ISMS and includes:

- Four phases of the PDCA cycle
- Standardization of all sub-processes included in the four phases of the PDCA cycle
- A catalogue including all security measures

Later in this paper we will research if these points could be used for the design and implementation of a DPMS. We can already mention that the main difference will affect the security measures, because these are quite different between IT security and data protection.

3.3. Standard Datenschutzmodell (Standard Data Protection Model)

The Standard Data Protection Model (SDPM) has been developed by Martin Rost, an employee at Unabhängiges Landeszentrum für Datenschutz (ULD), and is currently on its way to be implemented as standard in Germany for data protection controls and audits. The main points of this model consist in elaborating systems to evaluate data protection levels, both in private and public sector. These systems should research and evaluate the real situation of IT systems and informational processes in the sectors concerning compliance with data protection laws.[4]

This model is based on the following points:

4 Rost (2012), Standardisierte Datenschutzmodellierung.

- It establishes a list of data protection requirements guided by the protection targets (Schutzziele)
- It establishes a classification of the different components included in the organization's data processing. This classification is based on data, IT systems and processes
- It classifies the different kinds of data in three protection levels
- It works on the classification above, according to the protection requirements of different processes and IT systems
- It establishes a catalogue of measures to be applied in order to guarantee the required security/protection level[5]

The aims of protection are the classical/typical three of IT security: availability, integrity and confidentiality. The new (data) protection aims are transparency, unlinkability and ability to intervene.[6]

The data protection levels were developed according to the BSI (German Federal Office for Information Security) classification, and are the following three:

- Normal: Possible risks are predictable and eventual damages would be easily reparable
- High: Risks and possible damages would be significant and the affected subjects would need assistance in order to repair these damages
- Very high: Risks and damages that could be classified as catastrophic

The risk model establishes a catalogue of data protection risks that could be used for conducting a privacy impact assessment (PIA)[7]

- Risks of processes: This means the risk that could be generated for the data subject by a data process
- Model risk: This risk arises if a model cannot guarantee control according to the aims of protection mentioned above
- Risk of security measures: This risk arises when these measures do not exist or wrong measures have been chosen
- Risk of competences: This risk arises when the persons responsible for control and audit do not have the adequate competences to fulfill this task
- Compliance and control risk: This risk arises when the data subject is misled, thinking that an organization is compliant when it is actually not

5 Probst (2012).

6 Bock/Rost (2011).

7 Bock/Rost (2012).

3.4. COSO®

On 14 May 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a revised version of the framework «Internal Controls - Integrated Framework». The 2013er version replaces the old version of 1992, known as COSO® I, on 15 December 2014. Since 1992, COSO® is recognized by managements and supervisory authorities, regulators and professional bodies as an appropriate and comprehensive framework model for internal monitoring.

As operator of an IT infrastructure, it is indispensable to deal with numerous statutory provisions and their implications. Regulations always have, in an indirect manner, their effects on IT security. These provisions are summarized under the concept of corporate IT governance. Compliance with these regulations is very important, as non-compliance can result in heavy fines and liability obligations.

3.5. COBIT®

COBIT (Control Objectives for Information and Related Technology) was developed by ISACA, the international association of accountants, IS auditors, IT managers and executives from the top management level. Penned by ISACA derived COBIT® as a control framework for IT organizations with the focus on stakeholder needs (business needs), achievement of corporate goals through IT goals and the implementation of governance and business models for information security.

In 2012, ISACA published a revised framework COBIT® 5.0, wherein the areas of governance and management of IT processes have been extensively reworked. The main objective of COBIT® 5.0 is to better understand and to, as effectively as possible, map the needs of different stakeholders (stakeholder needs). Thus, COBIT ® 5.0 is a framework for control and management of IT organizations and IT companies and is used to increase efficiency in relation to the control of the IT organization processes. COBIT ® 5.0 does not expressly define how to implement requirements but primarily what shall be implemented.

3.6. ITIL®

ITIL® deals with the essential points needed for creating and running an IT service management organization. It answers questions about why a service-oriented, process-driven organization is necessary and how such an organization may best be achieved.

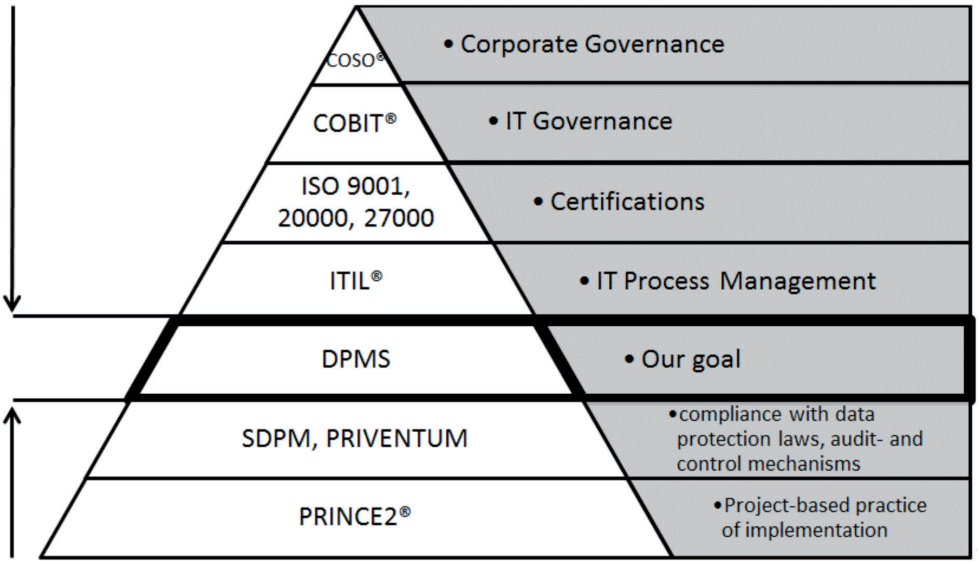
With structures that orient themselves on IT services, the IT organization realizes with ITIL® more efficiently good and even best practices. ITIL® offers countless possibilities for building up the organization and its processes. Thus ITIL® meets the demands of modern IT organizations, enables positive decision-making, and ultimately delivers value to the organization's business customers.

In times where resources are becoming tighter daily, IT organizations must use the means at their disposal as efficiently as possible, to monitor them, and as needed to correct and control the situation. The most vital of these aspects is an organizations customer orientation and the quality of its services.

3.7. Status Quo Summary

3.7.1. Illustration

The following graph illustrates the synergy of existing best practices.



3.7.2. Use of several and different systems

Nowadays there are almost no DPMS systems which really earn this name. We can find some software programs and standards trying to cover these services, but their only achievement is helping to manage data protection compliance requirements about IT security.

The ISMS Standards, like ISO 27001 or BSI Grundschutz currently are possibly the best chance, because they can help organizations learning to work in a systematical way. And, not to forget, they can solve problems about IT security, and IT security is, at least, part of the whole data protection issue.

3.7.3. Advantages and disadvantages

As mentioned above, the existing systems are not able to substitute a DPMS, but they could help to begin following the right track. For example, establishing an ISMS

cannot solve data protection management in an organization but it would help prepare the development of a DPMS. In the following we will point out a proposal for an adequate DPMS.

4. RECOMMENDED SET-UP FOR A DPMS

4.1. ISMS and DPMS: twins, but not identical

A DPMS should be closely connected with an ISMS and other established process frameworks, such as ITIL® and COBIT®, or methods of quality- and financial management and auditing. Therewith a data protection management can become a natural part of an organization. The abilities of a DPMS have to be enhanced in such a way that the DPMS is capable to check if frameworks that are latently interested in monitoring the performance assessment of employees actually comply with fundamental rights.

Despite the content-wise distance between DPMS and ISMS, a DPMS can adopt best components of an ISMS. But unlike, for instance compared to IT baseline protection («IT-Grundschutz»), no comparable standards have so far been elaborated regarding the examination of technical and organizational data protection measures of an ISMS, and left this task alone to risk indicators to measure the effectiveness of these measures. Privacy advocates apparently still underestimate the independent contribution of a DPMS. As consequence the motive of information security still dominates data protection.

4.2. Privacy by design, privacy by default and privacy enhancing technologies

An important prerequisite for the sustainable protection of personal data is the systematic use of the principle of Privacy by Design. The Commission´s proposal rightly emphasizes that companies should take, whilst collecting or processing personal data, appropriate technical and organizational measures to ensure a high level of protection of personal data. In order to support the application in as many sectors of the economy, Privacy by Design should therefore also be a mandatory criterion in the near future. Furthermore, for Privacy by Design as a state of the art not only implementation costs should play a role, but also the potential risks arising from the processing of personal data should be taken into account.

Overall, it must be ensured that Privacy by Design applies for the entire lifecycle of personal data. Systematic protection measures must be used, which ensure not only the accuracy, confidentiality, integrity and the physical security of personal data. In addition, the procedures for the erasure of data need to be considered and planned in the concept of Privacy by Design.Another important element of a DPMS is the sustainable protection of personal data through privacy-friendly default settings (Privacy by Default).

This means, as contained in the proposal of the Commission, ensuring by appropriate settings that only data is processed according to a specific purpose.

In addition, privacy-enhancing technologies (PETs), such as encryption or anonymization methods, depending on the context and the relevant risks of data processing should be made mandatory.

4.3. Risk management

Detailed impact assessments are the heart of any sustainable DPMS. Such assessments may be a bureaucratic burden on businesses but they guarantee that companies are becoming aware of the consequences of their data processing operations. If these impact assessments are carried out thoroughly, the likelihood of a data breach is considerably reduced.

Thus, data controllers should be forced to undertake a risk analysis to check whether a PIA must be carried out according to the requirements of the GDPR. The aim is to determine whether processing operations involve specific risks to the rights and freedoms of data subjects by their nature, their scope or their purposes. If one of these factors changes, the risk analysis should be updated.

For a more comprehensive protection of personal data, PIAs should take into account every step in the lifecycle of personal data. Accordingly, PIAs should, instead of general descriptions, contain a detailed description of the intended processing operations and the risks in terms of the rights and freedoms of data subjects risks and the planned corrective actions, guarantees, security arrangements and procedures by which evidence is to be given that the controller complies with the provisions of the GDPR.

The impact assessment must include a comprehensive data inventory, which describes number, type, and geographic scope, as well as the relevant purpose and context of the data processing. Additionally, it should be noted in detail in the impact assessment that privacy-friendly default settings or measures regarding the Privacy by Design principle have been implemented.

4.4. Compliance reviews

To ensure a sustainable protection, a schedule for the periodic review of compliance, so-called compliance reviews, should be set out in the impact assessment. According to the results of compliance reviews, impact assessments need to be adjusted if necessary.

These reviews only make sense if companies make sure that they actually keep the warranties set out in the reviews. The frequency of compliance reviews should be adequate with the context and the specific risks that may involve data processing operations. In addition, compliance reviews should be carried out immediately whenever the risks

to the rights and freedoms of data subjects change by their nature, their scope or their purpose for which they were collected.

Compliance reviews are primarily driven by the control of data protection measures and the above mentioned warranties given. However, they should also reveal whether the data controllers are sufficiently able to take into account the independent decisions of the persons concerned. Should the review identify inconsistencies, they must be mentioned in the compliance review, and suggestions for achieving full compliance should be made.

4.5. Information policy

A transparent and comprehensible information policy must be an essential part of any DPMS. Accordingly, companies should inform consumers as part of a comprehensive compliance mechanism on the data processing methods used.

Therefore, and to allow a faster understanding and a better comparability of data protection methods, once information has be made available the persons concerned, user-centric designs for easy-to-place privacy policies should be considered. Especially, since the use of smart devices and correspondingly displayed privacy policies on smart devices increase every day. To ensure innovative ways for the future, the icon-based privacy policy should be machine-readable, if it is provided in electronic form.

4.6. Implementation according to PRINCE2®

The ability of a company to be able to effectively and efficiently implement changes within IT architecture, especially within a DPMS; is critical to the future success of the company. The path from strategy to implementation is almost always a project-based way of doing.

The success of projects cannot be left to chance. A «hit-and-miss» approach carries too much risk, usually is more expensive and of poor quality, and resources are wasted. Successful projects may remain no single services, experiences must be secured.

An optimally adapted project management method such as PRINCE2® provides the controlled environment that allows the management to reliably set up projects and to delegate responsibility and authority. The PRINCE2® method also ensures that the required quality is delivered within a specified time frame and budget. PRINCE2® can be adapted to any size of project –whether it is a small DPMS, whose implementation timeframe lasts only a few days and includes only a few employees, or whether it relates to a large DPMS that needs a long time and a lot of project staff for implementation and integrates external suppliers. PRINCE2® could thus be a «best practice» method for the implementation of a DPMS.

5. FINAL RECOMMENDATIONS

5.1. General

From our point of view, the SDPM offers the best ground for the development of a DPMS, especially because it targets clearly legal compliance with data protection legislation, and also because it also focuses on the data subject perspective. According to SDPM criteria, a DPMS should

- clearly define which data processes are in place in an organization that could affect personal data. It should also inform about these processes to employees, Data Protection Authorities and data subjects,
- guarantee the unlinkability of data, assuring that the data can only be used for its original proposal,
- guarantee that the data subject can exercise its rights according to data protection legislation.

Because organizations have already great experience using ISMS, it will be useful to apply its criteria for the development and evaluation of a DPMS.[8] For this reason we will use the PDCA cycle criteria.

We really believe that a DPMS based on SDPM would be the best option in this field, and, to state a side note, professionally we are already working on the development of such a system.

5.2. Plan

- It is necessary to know the goals of each organization whilst implementing a DPMS, e.g. which data protection requirements the organization has to comply with, which profit should be achieved with the implementation and which the legal and organizational ground for this implementation is.
- It is necessary to define in which field the DPMS is about to be applied (normally in the whole organization) and regulate the relationship between ISMS and DPMS by defining the different fields of use.
- It is also essential to establish a clear system of risk assessment for the DPMS. This should be different from the ISMS, because in the field of data protection there are almost no acceptable risks, and this category is usually accepted in the IT security risk assessment.
- The organization should plan and organize training activities in data protection law.

8 Rost (2012), Faire, beherrschbare und sichere Verfahren.

5.3. DO

- Establish the DPMS guidelines
- Establish measures of risks assessment and management
- Define responsibilities
- Provide resources for implementation
- Planned training activities must be guaranteed
- Evaluating and auditing measures for the DPMS must be established
- Establish the risk management measures in a clear way; establish procedures to be followed between risk finding and applying measures
- SDPM protection measure should be used
- Organization should choose a process management system for the DPMS itself, the ITIL® criteria are probably the best practice
- All the points above should be properly documented.

5.4. Check

- Legal compliance of the DPMS with data protection law and of all the processes managed through the DPMS should be constantly evaluated
- Applied protection measures should be evaluable and evaluated
- Risk assessment should be constantly repeated
- DPMS should be regularly audited
- Organization's management should regularly evaluate the DPMS
- Resources planning, training activities, audits, data protection breaches, evaluation of protection measures and management evaluation must be properly documented

5.5. ACT

- Necessary improvements must be applied
- Corrections, preventive measures and improvement measures must be communicated within the organization
- Organization's management must control and evaluate all these measures

6. BIBLIOGRAPHY

Bock, K. / Rost, M. / (2011). Privacy by Design and the New Protection Goals - Principles, Goals, and Requirements. Retrieved March, 31st, 2013 from http://www.maroki.de/pub/privacy/BockRost_PbD_DPG_en_v1f.html.

Bock, K. / Rost, M. (2012). Impact Assessment im Lichte des Standard-Datenschutzmodells, In: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 10: 472-477.

Gerick, T. (2012). IT Analytics. Wege aus der Black Box. Retrieved March, 9th, 2013 from http://www.manageit.de/Online-Artikel/20120910/f%20IT%20Analytics.htm

Maseberg, S. (2012). Datenschutz Cert GmbH. Internal Document about Priventum Initiative.

Probst, T. (2012). Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444.

Rost, M. (2012). Faire, beherrschbare und sichere Verfahren, in: Kersten, Heinrich (Hrsg).; Peters, Falk (Hrsg.); Wolfenstetter, Klaus-Dieter (Hrsg.), 2012: Innovativer Datenschutz, Berlin: Duncker & Humblot.

Rost, M. (2012). Standardisierte Datenschutzmodellierung; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.

Weidenholzer, J. (2014). Retrieved March, 31st, 2013 from http://www.ots.at/presseaussendung/OTS_20140312_OTS0157/weidenholzer-weltweite-datenschutzstandards-setzen.

THE ABC OF ABC: AN ANALYSIS OF ATTRIBUTE-BASED CREDENTIALS IN THE LIGHT OF DATA PROTECTION, PRIVACY AND IDENTITY

Merel Koning
PhD candidate at the Privacy & Identity Lab, based at the ICIS Digital Security, Radboud University Nijmegen

Paulan Korenhof
PhD candidate at the Privacy & Identity Lab, based at Tilburg Institute for Law, Technology and Society (TILT)

Gergely Alpár
PhD candidate at the ICIS Digital Security, Radboud University Nijmegen

Jaap-Henk Hoepman
Associate Professor at the ICIS Digital Security, Radboud University Nijmegen, Scientific Director of the Privacy & Identity Lab

ABSTRACT: Our networked society increasingly needs secure identity systems. The Attribute-based credentials (ABC) technology is designed to be privacy-friendlier than contemporary authentication methods, which often suffer from information overspill. So far, however, some of the wider implications of ABC have not been appropriately discussed, mainly because they lie outside of the research scope of most cryptographers and computer engineers. This paper explores a range of such implications, shows that there are potential risks associated with the wider introduction of ABC in society, and makes the case that legal and societal aspects of ABC be subjected to extended interdisciplinary research.

KEYWORDS: Attribute-based credentials, Authentication, Identification, Data Minimisation, General Data Protection Regulation, Privacy by Design, Data Protection by Design, Socio-Technical Analysis, Legal Analysis.

1. INTRODUCTION

Technology mediates today's data-driven society in which the demands for secure and privacy-friendly digital identity management is growing. Scientist, industry and policy makers have –at least in the past– approached the privacy and security aspects of identity management as being a trade-off between the two. Cryptographic solutions, like attribute-based credentials (ABC), however, enable to build more secure and yet privacy-friendly identity management systems. National governments in the EU are

allocating funds to implement identity management systems and ABC make an interesting candidate. So far, however, there has been little discussion about the wider implications of ABC because they fall outside the normal research field of cryptographers and computer engineers. It has to be admitted that, despite good intentions, ABC implementations nevertheless still introduce a range of societal issues with regard to privacy and identity. Therefore, extended interdisciplinary research on the societal and legal effects of ABC is gaining in relevance.

This paper gives a technical and architectural overview of the ABC concept.

It will continue with an exploration of the reciprocal relationship between the self, identity construction, technology and the architectural decisions within an ABC ecosystem. Furthermore, the paper deals with questions regarding the extent to which an ABC system meets the legal concept of Data Protection by Design and Data Protection by Default.

2. AN OVERVIEW OF ATTRIBUTE-BASED CREDENTIALS

In most computer-related scientific work a digital identity is considered to be a set of characteristics describing certain properties about an individual. This set is dynamic, and depends on the context in which the individual is known. The attribute-based credential technology (Camenisch et al., 2011, Sabouri et al., 2012, Alpár & Jacobs, 2013) implements this model. Personal characteristics, such as age, name, social security number, credit card number as well as more mundane data, like hair colour and favourite dish, are called attributes in this model. Some of these attributes are not directly identifying (e.g. age or hair colour) whereas others are (e.g. name or social security number). [1]

In the conventional identity management model, identity providers are involved in retrieving authentic attributes. After user authentication, the identity provider retrieves and sends personal information about the user to the service provider. This process demands user identification and includes a trusted third party. For example: An individual can use her Facebook account to sign in to a Spotify account.

2.1. The ABC Characteristics

The ABC model stores attributes in a secure container called an attribute-based credential. This credential contains a predetermined set of attributes, whose values are determined by the characteristics of the individual user.

1 The identifying value of certain attributes led to the preference of ABC over the older term anonymous credentials.

Attribute values are reliably verified by an issuer o make sure they match the individual's characteristics. The issuer then secures the attributes in a credential by a digital signature. A municipality, for example, can issue a credential for the attributes of place of birth, residence, date of birth and certain age categories. Once some credentials are issued, the user can disclose a subset of her attributes to a service provider who requires certain information before providing a service. An online video rental store, for example, may need to verify that an individual is over 18 years old before allowing access to an age-restricted movie. Revealing this age category attribute 'I'm older than 18' is done via the mechanism called selective disclosure.

A typical selective disclosure process runs as follows: An individual user selects a service to access. The service provider sends a presentation policy (e.g, Camenisch et al., 2013) to the user asking her to reveal the value for a selection of attributes contained in one or more of her credentials. In order to protect against service providers sending overly broad presentation policies that ask for a non-proportionate selection of attributes, the policies are signed by a scheme authority prior to the selective disclosure process. Service providers can apply for the signature on a certain presentation policy at the scheme authority. They receive this signature after proving the relevance and proportionality of the set of requested attributes. During the selective disclosure process the user verifies this signature before accepting the presentation policy. The user subsequently decides whether she agrees to reveal all the requested attributes. In order to trust the values received, the service provider expects the credentials to be issued by known and trusted issuers. Sometimes, the system allows the user to choose to reveal only a subset of requested attributes. If the user refuses to reveal attributes, the service provider may choose to refuse the user's request, or offer only limited functionality.[2] Once all checks are done the attributes are revealed. Depending on the disclosed attribute values, the service provider can make an access decision.

2.2. The ABC Principles

From a technical point of view ABC must satisfy three requirements: unlinkability, confidentiality and security. The selective disclosure protocol uses zero-knowledge proofs as underlying privacy-enhancing technology (PET). Such zero-knowledge proofs allow a user to convince the service provider about the fact that she owns a credential, signed by the issuer, containing the attribute values disclosed, without showing the full credential itself to the service provider. The proofs achieve unlinkability: Given two proofs of ownership of a particular credential type, it should be impossible to determine (using the proofs alone) whether the same individual produced them or not. Clearly, this is trivial if an identifying attribute is revealed in the selective disclosure. Establishing a secure, encrypted, channel between the user and the service provider typically ensures

2 This is similar to what happens when users refuse to accept cookies or block website scripts.

confidentiality: Only the service provider learns the values of the attributes the user chooses to reveal, and she learns nothing more. For security purposes only the owner of a credential must be able to prove ownership of this credential. Even if several individual requests collude, a user should not be able to convince the verifier that she owns a credential that she originally do not possess. This is partially guaranteed by the fact that issuers sign credentials. This prevents rogue parties to create fake credentials. However, to prevent users to pool or share attributes in credentials, additional mechanisms are necessary. To this end, it is, first of all, assumed that each user has a private key, to which even the user is not privy. Secondly, credentials typically contain an expiry date. To improve the security, some ABC systems store the credentials on a smart card, and let the smart card compute the necessary zero-knowledge proofs.[3]

2.3. The ABC Use Cases

Attribute-based credential systems, especially when implemented on smart cards, can be used both offline and online. An example of an offline use case is the use of a tobacco vending machine. To prevent the sale of tobacco to minors, the vending machine can use ABC technology to verify that the buyer is over 18 (or whatever the appropriate legal limit is). For this to work, users must be able to obtain a credential from the municipality that contains an «over 18» attribute. When buying cigarettes the user inserts her smart card in the vending machine and proves she is over eighteen and from there on continues the purchase transaction.

A typical example of an online use case for ABC is verifying whether a user is subscribed to an online service (such as a digital newspaper or Netflix). These service providers demand strong guarantees that only paying costumers can access the content. With the ABC technology the service provider can issue a credential with an attribute of the type of subscription for every new subscriber. This attribute does not need to contain a membership number (thus, not identifying); access to content can be decided on the type of subscription after the zero-knowledge proof. In this example the service provider is both a credential issuer as well as a relying party towards the attribute.

2.4. The ABC Ecosystems

Scheme authorities play an important role in attribute-based credential schemes. They are responsible for keeping the scheme trustworthy to all stakeholders. Trust is maintained by having a clear policy, describing the roles and responsibilities of all participants in the scheme, and by effectively enforcing this policy. The scheme authority has the power to do so because it can decide

3 For example, the IRMA project (https://www.irmacard.org).

- which issuers are members of the scheme,
- which credentials/attributes a particular issuer can issue,
- which service providers are members of the scheme,
- which credentials/attributes a particular service provider is allowed to access, and,
- which users are issued a card.

These five powers are enforced by the ABC technology. The party that functions as the scheme authority, and the policy that it defines has a major influence on the trust and functionality of the corresponding ABC system. We call a particular instance of an ABC scheme with a certain policy an ecosystem. Several ecosystems can coexist

One possible ecosystem is a national eID system where a government agency is a scheme authority, and whose policy restricts the use of such an eID to government only issuers and service providers. Such a top-down ecosystem has a restricted functionality, but most likely a high level of trust among the service providers while perhaps having a lower level of trust (in terms of privacy) among particular group of users.

A more flexible ecosystem is created by also allowing private sector use of such a government issued eID card. Companies can then serve as issuers and service providers. This hugely increases the number of possible applications of the eID card, but perhaps lowers the overall trust in the system.

Bottom-up, private sector based, approaches are also possible. For example, different companies can decide to issue ABC cards that conform to a certain industry standard that allow arbitrary issuers and service providers to use the platform. In essence in such a setup, no scheme authority is present at all. But small groups of stakeholders may decide to create a scheme authority of their own and use the open platform to create a more closed ABC subsystem. Multiple ABC schemes then coexist on a single card.

3. THE SOCIO-TECHNICAL ASPECTS OF ABC'S

The following section will assess the socio-technical aspects of the techniques discussed above. In today's society authentication is of great importance. Often legal or security rules require individuals to prove certain attributes. Take, for instance, the example of buying tobacco in the previous section. Without an ABC system an individual has to show an ID card to prove the «over 18» attribute, yet these IDs show additional, non-necessary attributes, like date of birth, name, place of birth, gender, etc. Showing additional, non-necessary attributes can be considered an information overspill and gives rise to privacy concerns.

Privacy plays a crucial role for the autonomy of individuals with regard to their identity management (cf. Goffman, 1959). Often, privacy is described in terms of control over personal information. The legal scholar Westin defines privacy as «[...] the

claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others» (Westin, 1966, p. 7). The information scientist Agre defines the right to privacy as «the freedom from unreasonable constraints on the construction of one's own identity» (Agre, 1998, p. 7). A lack of privacy can deprive individuals of choices concerning their self-presentations and the types of social relationships they can establish (Rössler, 2001, p. 112). Privacy breaches can therefore restrict an ndividual in her autonomy to develop her own identity and determine her life plan (Kupfer, 1987, p. 82).

ABC can limit the information overspill. By, for example, only revealing to be over 18 instead of revealing all information on an ID card, ABC systems give technologically dictated privacy safeguards. The selective disclosure of attributes can be an effective means to battle discrimination and aid individuals to control their information.[4] To a certain extent an ABC system improves the autonomy with regard to revealing personal information in different contexts.

Despite these promising facts, ABC form a technology and as such it actively co-shapes the environment in which it is deployed as well as the way individuals relate to one another (cf. Verbeek, 2005). In this capacity ABC systems are interesting to extensively reflect on from a non-technical view. An ABC card is not just an artefact; one cannot simply «use» it. The technology of the ABC card is «a sociotechnical system of use», «a system using combinations of hardware and people (and usually other elements) to accomplish tasks that humans cannot perform unaided by such systems» (Kline, 1985, p. 210-211). The ABC technology is an artefact that reveals whether an individual has or does not have a certain attribute, this is something that without the aid of any artefacts (including ID cards) people are not able to accurately perceive for a majority of attributes. The effects of a new technology cannot be easily predicted until the technology is extensively deployed (Collingridge, 1980). However, due to the potential of ABC in a (future EU obligatory) eID system, we do want to anticipate on the possible impact of ABC on one's autonomy. We will focus on ABC implementations on smart cards.

3.1. Attributes: the 'Haves' and 'Have Nots'

Labelling individuals with certain attributes and others not, could have benefits for both individuals and society in several contexts.[5] The ABC technology provides for an easy means to do so. However ABC technology may not only provide others with

4 E.g. persons who are questioning or experimenting with their gender may not want to share their current legal genderstatus, which may differ from their social identity.

5 See for instance Liagkou, et al. (2014). As the title suggests, this paper is a summary of ABC-4Trust's Greek pilot's setup (results are not included yet). This paper includes a general discussion about the dangers of ABC applications in public opinion polls without thorough analysis

information (individual A has or does not have attribute B) – but it also 'shapes' the information and the manner in which it is experienced. Throughout history people use technology to view the world in a fashion to which they are not capable to do so without the mediation of technology, and in return technology may co-shape the manner in which individuals perceive and interpret themselves and their world (Ihde, 1983, p.22). For instance the use of a thermometer: people cannot feel 'degrees' as such and can only perceive it with the use of this artefact. In return the technology mediates our self-interpretation and interpretation of others. Some people use the thermometer as a decisive factor to regard oneself as ill or verging on ill.

Since the ABC technology sees on identity management, it is important to raise the question how an ABC system would affect the manner in which individuals interpret their identity and that of others. Will this privacy-enhancing technology (PET) lead to a culture in which the individual becomes a 'have' or a 'have not' of certain attributes? ABC systems could potentially be a foundation for the use of overformalized personae because the individual gets access to certain services based on a black-and-white scenario: either one has the attribute or one does not have the attribute. This scenario ignores the –often spacious– gray area between these two extremes, in which many factors play a role in self-interpretation. The types and value options of attributes are therefore of the utmost importance. For instance, with regard to gender Australia recognizes gender X. When an ABC ecosystem only recognizes the attribute values 'female' or 'male', individuals with gender X are limited in their identity-construction in the ABC ecosystem and will be forced to 'fit' into the options offered by the ecosystem. For attribute types and values individuals will be highly dependent on the discretion of the scheme manager and issuers. Thus, the discretionary power of scheme managers and issuers has a far-reaching influence on the autonomy of individuals to shape their identity. An individual cannot 'be' what is not recognised as an attribute in the ecosystem. In return, the attributes allocated to a specific individual can have a reflexive effect with regard to that individual's self-interpretation. For an individual it generally is important to be recognized by others in correspondence with her self-identity. The sociologist Giddens points out that self-identity «has to be routinely created and sustained in the reflexive activities of the individual» (Giddens, 1991, p. 52). This reflexive self-interpretation could be influenced by the allocation of attributes and the continuous confirmation of such attributes within an ABC ecosystem. The result could be that people end up modelling themselves «upon their own artefacts. (...) The creator interprets himself through the created» (Ihde, 1983, p. 74). When thinking of this in the light of potential obligatory use of ABC cards for a wide range of purposes in a wide range of contexts, the question rises whether individuals would start to define themselves and human traits in

and shows that attributes may be important when authenticating for an opinion gathering (polls).

general within the limits of the types and values of attributes recognized within an ABC ecosystem. Even if a wide range of attribute types and values is recognized, the ABC technology still dictates a black-and-white decision; the individual has or does not have a particular attribute, and on this base further decisions are made.

3.2. Function Creep

Technology can be developed for a particular use or purpose. However, oftentimes the technology allows for deployment for other purposes. There is no reason to exclude the applicability of this phenomenon to technology that is initially developed for privacy safeguarding purposes, such as ABC. Technology generally promotes or provokes a specific kind of use (Verbeek, 2005, p. 115), which can stray from the ideas behind the technology.

ABC cards are a technologically dictated reliable source of information and are promoted as 'privacy-friendly' (Camenisch et al., 2010, 2011). An ABC card is much less intrusive than requesting an ID document, e.g. a passport. Businesses and government institutions will –most likely and to a certain extent– encourage its wide range of use, because it is a reliable source of authentic information that they want or need. These entities will be inclined to use ABC to lessen the chance getting accused of privacy-infringements as they use a 'privacy-friendly' technology. As a consequence, more services may ask for an ABC card and attributes. Once there is a nationwide infrastructure supporting ABC[6], and once a large fraction of citizens owns an ABC-like card that is accepted by the majority of businesses and government institutions, the use of this card may become mandatory. Additionally, the cost for asking more information than is strictly necessary is essentially zero. This could lead to the regulation of instances in which a service provider must or may ask for ABC. An individual could then be forced into a position in which she has to identify or authenticate herself in a context in which she previously did not have to do so. ABC can thus have the reverse effect with regard to the initial design idea. This could increase the risk of being profiled; service providers may allow or reject access to certain services based on a small set of attributes. This might lead to discrimination in a new 'jacket'; attribute-based discrimination.

3.3. Authentication Obstructs Obfuscation

Currently there are situations in which an individual does not have to prove her identity in order to get access to a service. For instance, when buying a book online, paying and providing a valid shipping address will generally lead to a successful transaction.

6 E.g. Spirakis & Stamatiou (2013) suggest that the ABC technology will ultimately replace traditional PKI in the context of citizen identity.

However, users are typically required to create an account to finish the transaction. Except for relevant details (like shipping address), people can and do provide fake information for irrelevant account data. Another example is the situation in which an individual wants to get access to a 'personalized' discount card of a grocery shop. Signing up for such a service with an obfuscated identity generally does not hinder the card issuance. In other words, in the current landscape the individual can obfuscate some information without disturbing the service delivery.

ABC cards might influence users in their obfuscation behaviour. Due to the privacy-friendly image of ABC, the urge to obfuscate an identity can decline. However, by using an ABC system, individuals are no longer given a choice to autonomously decide if and what characteristics of their identity they will obfuscate. The consequences of the implementation of ABC systems could be that services like Google and Facebook will have a foolproof way to enforce a real-name policy (Alpár & Jacobs, 2013). Similarly, age-restricted content is truly out of reach for minors. This removes any discretionary decision space for parents (to allow their children access to age restricted content, such as computer games, where the age limit is often set by companies in countries that are different from the age constraint typically enforced in the country of origin), or whistle blowers, researchers or journalists (that would like to use some services without revealing their full name). Over-implementation of an ABC system would diminish individuals their autonomy by depriving them of choices with regard to the manner in which they present themselves or use a pseudonym etc. in several kinds of interactions. Individuals will have to adhere to the norms of the service providers and are left little means to circumvent or negotiate these norms; their behaviour is regulated by technology (cf. Leenes, 2011).

4. ABC'S AND DATA PROTECTION BY DESIGN AND BY DEFAULT

The following section will analyse the compatibility of an ABC system with the concept of Data Protection by Design and Data Protection by Default (DPbD) as proposed in EU Data Protection Regulation. We will focus on the data protection regime as laid down in the European Union.[7] At the time of writing this paper the Regulation[8]

7 Data processing for purposes that fall outside the scope of the jurisdiction of the EU and data processing for criminal law enforcement purposes fall outside the scope of this paper.

8 The Draft version that is used to write this paper is: Report A7-0402/2013 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Date: 21.11.2013. We will refer to this version as: GDPR.

is still in the making. However, despite the fact that the concept of DPbD is not (yet) substantive law, an analysis can be interesting for multiple reasons. Firstly, DPbD can be considered to be the legal obligation to implement privacy-enhancing technologies, such as ABC. Secondly, DPbD relates to the data protection standards as set in article 5(1) sub a of the General Data Protection Regulation (GDPR). These data protection standards date back to the early eighties when they first appeared in international treaties.[9] By testing to these principles, the ABC technology is assessed against the core of the current data protection doctrine. Thirdly, the ABC technology invites the increased usage of pseudonymous data. The GDPR introduces an innovative 'data protection light' regime on pseudonymous data processing. Analysing the legal conditions DPbD could contribute to a better understanding of the privacy enhancement of this technology. Due to the word restrains we will focus on those aspects of DPbD that relate to the sociotechnical aspects.[10]

4.1. The General Obligation of DPbD on the Data Processor

The data protection framework regulates personal data processing. The scope of the term data processing includes any operation that is performed upon personal data, whether or not by automatic means.[11] The term personal data refers to any information relating to a directly or indirectly identified or identifiable natural person.[12] The data protection framework, therefore, does not regulate the design phase of the systems that can process personal data. Knowing this, the EU commission called upon system designers to take responsibility -from a societal and ethical point of view- for the data protection aspects in their systems back in 2007.[13] On top of this appeal and in hope that the data protection standards will permeate into the entire design chain, the EU legislator now introduces DPbD. This new concept lays down a general obligation on the data controller to implement appropriate technical and organizational measures

9 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available on http://www.oecd.org/internet/ieconomy/oecdguidelines ontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Last retrieved on 10 March 2014. EC-Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing C60/48 13 March 1975; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108; Directive 95/46/EC.

10 Further research on the ABC and DPbD is suggested.

11 GDPR article 2 sub b. This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

12 GDPR article 2 sub a.

13 Privacy Enhancing Technologies (PETs) European Commission - MEMO/07/159 02/05/2007.

within the entire life cycle of the technology to ensure data processing to meet the data protection standards.[14]

As explained in the technical overview of ABC, credentials can contain identifying and non-identifying attributes. It follows that when directly identifying attributes are issued or revealed, the issuer or service provider is processing personal data and the Regulation would apply. In case the presentation policy asks for a set of isolation-regarded non-directly identifiable attributes but the combination of the values or the combination with other non-ABC data is identifying, the Regulation also applies. In case the attributes requested in the presentation policy are not directly identifiable and the context allows for certain 'anonymity', the data is anonymous and the Regulation does not apply. In the coming sections we will focus on the processing of personal data. In an ABC ecosystem the issuers and the service providers should be regarded as the data processors: they determine the purposes and the means of the data processing. These entities must ensure the data protection standards and should implement appropriate technical and organizational measures. The substance of DPbD and the data processing standards will be assessed in the coming sections followed by the assessment of the extent to which ABC meet the DPbD obligation.

4.2. The Data Protection Standards

DPbD should be taken into account at the moment of determining the purposes and the means of the data processing as well as at the time of the actual data processing itself. During the entire lifecycle of the data there should be a consistent focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. The policy requirements of Data Protection by Default should safeguard that only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.[15] In the latest version of the GDPR article 23(1) lists the conditions that should be taken into account while implementing the technical and organizational measures. These include: the state of the art current technical knowledge, international best practices and the risks represented by the data processing. The data protection standards are formulated in article 5(1) sub a GDPR. They consist of the general instruction to only process data in a lawful, fair and transparent manner.

14 Recital 61 GDPR.

15 Article 23 GDPR.

The lawful processing standard is embodied by the criterion of legitimate purposes of article 5(1) sub b GDPR. This criterion must be explained in terms of a substantive conception of legality.[16] It does not only refer to the limitative enumeration of legal grounds on which data can be processed in accordance with article 6 of the GDPR, but also to the data controller's duty to determine the purposes and to process personal data in accordance with the law, state-of-the-art techniques and cultural and societal norms.[17] This criterion requires besides a legal assessment, a technology assessment, and hence has a potential propelling effect on the actual implementation of technological innovations. The processing grounds of article 6 GDPR should be obtained prior to –or at the latest at the moment of– the processing of the personal data. At least one of the limitative processing grounds should apply; these grounds vary from consent to a balancing act between the legitimate interests of the data processor and the fundamental rights of the data subject.[18] Consent should be a freely given specific and informed indication of the data subject's wishes.[19]

One would expect an ABC process to be bases on the legitimate ground 'consent' because the user can agree or disagree with the presentation policy.[20] However, as explained in section 2.1 the service provider is entitled to refuse the services in case the data subject does not agree to reveal all attributes that are requested in the presentation policy and the discretionary power of the user to lie about attribute values is limited (section 3.3). One could therefore question whether the ABC systems can process data on basis of consent in all instances; when the alternative is «no service» the freeness of the indication of the data subject's wishes is doubtful.

The purpose limitation principle sets a precondition and demands personal data to be collected for specified, explicit and legitimate purposes (purpose specification) and not to be further processed in a way incompatible with those purposes (use limitation).[21]

---

16 This broader conception connects the processing grounds to the aspect of foreseeability of article 8(2) European Convention on Human Rights; in the case of interference with the right protected under article 8 there have to be clear, detailed rules specifying the conditions subject to which interferences are legitimate.

17 Article 29 Working Party Purpose Limitation 2013 WP 203.

18 Article 6 a-f GDPR.

19 Recital 25 GDPR.

20 Article 6 sub a GDPR.

21 Use limitation prohibits the further processing of data in case the processing purposes are incompatible with the purposes at the time of the data collection The article 29 Working Party proposed a test in which the relationship of the purposes, the reasonable expectations of the data subject, the nature of the data, impact of the data processing and the safeguards must be weighted in order to determine the compatibility. Article 29 Working Party Purpose Limitation 2013 WP 203, p. 21 and 40.

This principle is of central importance to the whole data protection framework because it fulfils a conditional function for the interpretation of the other fair processing principles, such as adequacy, relevance, proportionality, accuracy, completeness and duration of retention. Like the processing grounds, the purposes need to be specified prior to, and in any event, not later than, the time when the collection of personal data occurs.

The purpose of the use of ABC cards within a particular ecosystem is to a large extent determined by the scheme manager who determines what attribute types are recognized. The issuer decides about the variations in value. These variations determine the possibility for further use too. Take for example the values in the 'gender' attribute from the previous section. The knowledge of gender X can be valuable for further processing for marketing or medical research purposes. The policy aspects influence the further use and purposes. Personal data can only be processed if, and as long as, the purposes cannot be fulfilled by lesser means, such as processing information that does not (directly) involve personal data: pseudonymous data or anonymous data. DPbD also sees on the storage minimization principle: «[P]ersonal data must be kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.»[22]

The ABC technology hardcodes the data minimization principle. Once the scheme manager determined what is proportionate and necessary (within the limits of the Regulation) and approves the presentation policies, the data processed for one purpose is minimized to the authorized attribute types coded in the presentation policy. However, as mentioned in the previous section on the socio-technical aspects, function creep is a potentially serious issue for ABC. Since ABC are generally perceived as a privacy-enhancing technology and the system provides strong authentication and a 'good image', societal over-use could be a potential threat to the data processing minimization principle. Besides this, the selective disclosure protocol of ABC empowers the data subject to control the first release of the personal data, however, after that first release the user is just as dependent on the service provider with regard to further use of the data as the subject is in current data processing. Further distribution of the data is not technically regulated by ABC systems and must be regulated by additional policies.

4.3. Pseudonymous Data and Profiling

The GDPR proposes a special 'light' regime on the processing of pseudonymous data.[23] Pseudonymous data should be distinguished from anonymous data, which is information that does not relate to an identified or identifiable natural person. The

22 Article 5(1) sub e GDPR.

23 See Diaz et al. (2008) for an assessment on eID systems and the current legal framework on pseudonymous data.

principles of data protection do not apply to anonymous data. Article 4(2) sub a GDPR defines pseudonymous data as personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution. This light regime particularly affects the legal regime on profiling: forms of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[24] Profiling based solely on the processing of pseudonymous data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject.[25] However, when profiling –whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources– permits the controller to attribute pseudonymous data to a specific data subject, the processed data is no longer considered to be pseudonymous.[26]

The use of ABC could have propelling effect on profiling. As described in section 3.2, 3.3. and 4.2 ABC can have a stimulating effect in terms of the quality of data that is revealed (paragraph 3.2 and 3.3) and the quantity of the data processing (3.2 and 4.2). Pseudonymous data is often used for big data and predictive analytics for profiling and targeting purposes. Profiling on the basis of this type of data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject. However, one could question whether profiling with pseudonymous, but verified authentic attributes, will -in the long run- not affect the interests, rights or freedoms of the data subject. With an ABC system the data becomes more valuable and the technology does not regulate the combination or further use of attributes; neither do the policies. The proportionality assessment for the other purposes or further use for which the data might be collected via the ABC card, does not lay in the hands of the scheme manager because this entity only assesses the proportionality with regard to the authentication problem.

---

24 Article 20 GDPR.

25 Recital 58 a GDPR.

26 Recital 23 GDPR states: The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. Art 10 lid 1. If the data processed by a controller do not permit the controller or processor to directly or indirectly identify a natural person, or consist only of pseudonymous data, the controller shall not process or acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

5. REMAINING ISSUES

When it comes to implications of ABC the sections above are far from comprehensive. In this section we intend to collect further problems that can arise while designing, deploying and operating an ABC system. The technical countermeasures to these potential issues are out of scope in this work because of space limitations and the socio-technical and legal focus of the current research.

A serious security and privacy threat is formed by the user herself. In general, a user is the weakest link of systems security. ABC give the user control and with that more responsibility. For instance, by choosing an easy-to-guess PIN that authorises transactions with service providers, a user risks the protection of her card. Another danger is social engineering that may enable malicious parties to capture the PIN or even the ABC card itself.

In order to have effective control, users should be empowered to check their attribute values. A user-friendly way to do that is by means of a computer or smart phone. This function should be safeguarded by a PIN or biometrics. In spite of the protection a computer or a smart phone is highly untrusted and identity theft via the ABC user panel is not unthinkable. Depending on the ecosystem this attack can become a 'one-stop-shop' for cybercriminals. Moreover, because an ABC card stores a valuable collection of authentic personal data, the business incentive to develop malware (e.g. keylogger, trojan) to acquire these attributes is even bigger.

Malicious activities can also occur on an infrastructural level. Even though an attribute may be anonymous, the 'leaking' of information from another level in the infrastructure, such as an IP address, could make the attribute pseudonymous or even fully identifying; consider for example, the nationality attribute with value 'Australian' in combination with IP address 82.165.102.217. [27]

From an organizational point of view the trustworthiness of the scheme manager is hard to determine. The anonymous aspects of ABC make it even harder to audit the transactions and schemes. Although several revocation techniques have been suggested (Lapon et al., 2011, Hajny & Malina, 2013), the revocation of attributes is still difficult because of the intractability of certain ABC transactions coupled with efficient implementation and proper security (Alpár et al., 2013).

But the utmost difficulty for ABC has to be the mismatch between the idealism behind the technology and the current data-driven society. Personal data is considered the 'new currency' and without an ethical change the data processing practices will most likely not change. Connected to this issue is the nature of humans: people want to share

27 The IP address of the Embassy of Ecuador in London.

data. There are yet to find sufficiently appealing business cases for ABC that compete with the current data processing practices.

6. CONCLUSIONS

Like the legislators in Collingridge's dilemma, we too «face a double-blind prob- lem: the effects of the new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change.» [Collingridge, 1980]. Our attempt was to indicate a set of issues that are likely to arise and –at least– should be given thought before implementation of an ABC ecosystem in society. ABC should be regarded as a socio-technical system that requires co-existence of human and machine. The effects of hard attributes on self-interpretation, the view of others and reflexive self-interpretation should be taken into consideration when assessing this technology. Attribute-based credentials limit the information overspill. But, as described in this paper, this technology does not limit data processing. Due to its privacy-friendly image and verified high quality of data, prompt broad deployment of ABC seems tempting.

However, one could conclude that ABC might have a reverse effect with re- gard to the initial design idea because broad deployment in various contexts may result in stricter authentication than the current practice. The use of ABC cards hinders an individual's strategy in identity obfuscation and the use of fuzzed attributes. ABC diminish the possibility to lie and make informal social agreements. The initial privacy-friendly intent influenced the technical design, but the technical design now influences the 'further' processing purposes. Because of the authenticity of the data and the data protection 'light' regime on pseudonymous data, there is a high probability that information from the ABC will be further used for profiling purposes. In the long run this can affect the rights and freedoms of the data subject. Despite the stimulus data processing for further use might receive from ABC, the technical and policy scheme of ABC only regulates the first use and the proportionality for this initial purpose. Therefore, ABC can be considered 'data protection by design' but they should not by default be considered data protection by default because many aspects are either not covered by the technology or depend on the grace of the scheme manager.

7. BIBLIOGRAPHY

Agre, P.E. (1998). Introduction. In P.E. Agre and M. Rotenberg (Eds.), Technology and privacy: The new landscape (3rd ed., pp. 1-28). Sabon: The MIT Press.

Alpár, G., & Jacobs, B. (2013). Credential design in attribute-based identity management. In Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference (pp. 189-204).

Alpár, G., Hoepman, J. H., & Lueks, W. (2013). An Attack Against Fixed Value Discrete Logarithm Representations. IACR Cryptology ePrint Archive, 2013, 120.

Camenisch, J., Mödersheim, S., Neven, G., Preiss, F. S., & Sommer, D. (2010, June). A card requirements language enabling privacy-preserving access control. In Proceedings of the 15th ACM symposium on Access control models and technologies (pp. 119-128). ACM.

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., & Zwingelberg, H. (2011). D2. 1 Architecture for Attribute-based Credential Technologies–Version.

Camenisch, J., Dubovitskaya, M., Lehmann, A., Neven, G., Paquin, C., & Preiss, F. S. (2013). Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. In Policies and Research in Identity Management (pp. 34-52). Springer Berlin Heidelberg.

Diaz, C., Kosta, E., Dekeyser, H., Kohlweiss, M., & Nigusse, G. (2008). Privacy preserving electronic petitions. Identity in the Information Society, 1(1), 203-219.

Giddens, A. (1991). Modernity and self-Identity: Self and society in the late modern age, Standford: Stanford University Press.

Goffman, E. (1959). The Presentation of Self in Everyday Life. London: Penguin Books (used print: 1990).

Hajny, J., & Malina, L. (2013). Unlinkable attribute-based credentials with practical revocation on smart-cards. In Smart Card Research and Advanced Applications (pp. 62-76). Springer Berlin Heidelberg.

Ihde, D. (1983). Existential technics. New York: State University of New York Press.

Leenes, R. (2011). Framing techno-regulation: An exploration of state and non-state regulation by technology. In Legisprudence, 5: 2, p. 143-169.

Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C., Spirakis, P., & Stamatiou, Y. C. (2014). Privacy Preserving Course Evaluations in Greek Higher Education Institutes: An e-Participation Case Study with the Empowerment of Attribute Based Credentials. In Privacy Technologies and Policy (pp. 140-156). Springer Berlin Heidelberg.

Kline, S. J. (1985). What is technology?. In Bulletin of Science, Technology & Society, 5(3), 215-218.

Kupfer, J. (1987). Privacy, Autonomy, and Self-concept. In American Philosophical Quarterly 24 (1):81 - 89 (1987).

Poller, A. Waldmann, U. Vowé, S., Türpe, S., (2012). Electronic Identity Cards for User Authentication-Promise and Practice. In Journal IEEE Security and Privacy, Volume 10 Issue 1, January 2012 (pp. 46-54).

Rössler, B. (2001). Der Wert des Privaten. Frankfurt am Main: Suhrkamp Verlag (used print: English translation, Cambridge: Polity Press, 2005).

Sabouri, A., Krontiris, I., & Rannenberg, K. (2012). Attribute-Based Credentials for Trust (ABC4Trust). In Trust, Privacy and Security in Digital Business (pp. 218-219). Springer Berlin Heidelberg.

Spirakis, P., & Stamatiou, Y. C. (2013). Attribute Based Credentials Towards Refined Public Consultation Results and Effective eGovernance. In Cyber Security and Privacy (pp. 115-126). Springer Berlin Heidelberg.

Verbeek, P. P. (2005). What things do: Philosophical reflections on technology, agency, and design. University Park, Pennsylvania: Pennsylvania State University Press.

Westin, A. F. (1970). Privacy and freedom. New York: Atheneum.

THE RIGHT TO READ ALONE
A dimension of privacy and a democratic challenge

Cédric Goblet
Lawyer at the Brussels Bar

«In solitary reading, the man in search of himself has some chance of finding what he seeks.»
(G. Duhamel, extract from *Défense des Lettres*)

ABSTRACT: Information and communications technologies provide means to monitor individuals' reading habits in an unprecedented way. In an age of e-books, tablets and e-libraries, the reader comfortably seated in his armchair is no longer alone; and it becomes almost impossible to select reading material anonymously. Digital content publishers and retailers are now able to collect and process very detailed information about readers: the search terms we use to find books, the amount of time we spend on a given page, what we have read in the past, how we engage with particular works, and when we get bored. Even annotations and highlights are analysed. All these data open a window into the reader's thoughts, opinions and feelings.

In this paper, I propose to define the right to read alone as the freedom to access, select and assimilate written materials without any kind of scrutiny or any form of surveillance from the State or private companies. I argue that this right is a dimension of privacy.

For a long time, people could ensure this right was respected by carving out for themselves an intimate space in which to read. Now, as the online environment has led to the disappearance of the frontier between private and public spaces, we will see how personal data protection principles may operate to ensure this essential freedom. The data protection regulation currently in force at both European Union and Council of Europe levels will be examined.

This study will also give us the opportunity to explore how the right to read alone interacts with the right to receive information, as well as with freedom of expression and of thought. I will demonstrate that there is a close interdependence of these fundamental rights, and conclude that the protection of readers has an impact not only on the ability to exchange information in a society, but also on our intellectual freedom and creativity.

KEYWORDS: Right to read alone, Reading activity, Readers, E-books, E-libraries, Privacy, Personal data protection, Freedom of expression, Freedom of thought, Right to receive information, Directive 95/46/EC.

1. PROTECTING READERS' FREEDOM: AN INCREASING CHALLENGE FOR DEMOCRACY IN THE 21ST CENTURY

States and religious authorities have always sought to control the information available to the public, and especially the circulation of written materials, be they books,

newspapers or pamphlets. The level of restriction and of respect for freedom to access information depend on the nature of the political regime in place. Undoubtedly, this control differs between a democratic country and an authoritarian one, in intensity as well as in the methods employed. However, in both situations, the control operates in two ways. Firstly, information flow can be restricted by acting at the level of the *transmitter*, in other words when the idea or the opinion is expressed, recorded in some medium and disseminated. The second way consists of monitoring and repressing the *receiver*, and especially the reader when it comes to written content.

Traditionally, those holding power have almost entirely concentrated their efforts on the *transmitter*. We are all aware of the long list of authors arrested and sentenced by judicial authorities, as well as the number of works censored, blacklisted or burned throughout history. The *receiver*, on the other hand, largely escaped the wrath of the authorities, since the technical means to control their intellectual activity were rather limited. This is not to say that readers enjoyed more freedom or that they were free from scrutiny. Various cases may indeed be found in the past where readers were prosecuted and sometimes sentenced to death[1]. However, the number of *receivers* upon whom sanctions were imposed is certainly less significant than the corresponding number for *transmitters*.

Today, the development of information and communication technologies has progressively led towards a reversal of this situation. A trend is emerging whereby information is controlled by taking steps directly against the *receiver*. Where formerly the control of readers was marginal, it will gradually become pervasive. Several factors explain this tendency.

To begin with, we should keep in mind that, for centuries, the majority of the population was illiterate and that books were luxury objects. As Martyn Lyons explains, significant advances towards general literacy were made in the Age of Enlightenment. They continued later on, so that the end of the 19th century was *«the golden age of the book in the West»*[2].

In addition, the Internet has considerably reduced the possibility of restricting freedom of expression and of having any practical effect on the *transmitter*. The reason is that thanks to this new medium, information can be duplicated easily, and shared quickly with a broad user community, as well as transferred from one location to any other on the planet in just a few clicks. While censors are generally only able to operate within national borders, the Internet has a worldwide dimension.

By contrast, new technologies - including naturally the web - provide means to monitor individuals' reading habits and intellectual activity in an unprecedented way. Tota-

1 See, e.g., Ginzburg, C. (1980). *The Cheese and the Worms - The Cosmos of a Sixteenth-Century Miller*. Baltimore : The Johns Hopkins University Press.

2 Lyons, M. (1999). *New Readers in the Nineteenth Century : Women, Children, Workers.* In Cavallo, G. & Chartier (dir.), R. *A History of Reading in the West.* Amherts: University of Massachusetts Press, p.313.

litarian regimes may now repress political dissidents and track unconventional thoughts with a fearsome efficiency. Private companies in the electronic book sector use technical means that would have been beyond the grasp of even the craziest dictator a short time ago. They collect very detailed information about our tastes, desires, emotions and opinions in gigantic databases. As all this data is available, State authorities may be tempted to request access to it for various purposes. This poses a severe threat to our fundamental rights and individual freedoms.

It should not be thought that such violations never occur in advanced democracies. «*Not only totalitarian governments fear reading*», observes Alberto Manguel. «*Almost everywhere, the community of readers has an ambiguous reputation that comes from its acquired authority and perceived power*»[3].

Americans remember the McCarthy hearings in the 1950s, where people were questioned on whether they had read Marx or Lenin; and whether their friends, spouses or associates had books about Stalin on their bookshelves[4]. «*Imagine if social readers had existed during the McCarthy era*», observes M. Kaminsky: «*the government would have been able to check each person's virtual bookshelf for blacklisted material*»[5].

More recently, in the years since September 11, the FBI has used its expanded power under the USA Patriot Act to request libraries' records on their users. The American Library Association estimates that between 2001 and 2005, more than 200 libraries were contacted by law enforcement agencies seeking information on reading habits and books borrowed[6].

Given this new surveillance environment, it becomes vitally important to examine the way our legal system ensures free access to information, as well as the development of independent and critical thought. When defining safeguard mechanisms, particular attention must be drawn to the rights of *receivers*, and especially to the protection of their privacy and personal data.

In this research, I propose to define the right to read alone as the freedom to access, select and assimilate written materials without any kind of scrutiny or any form of surveillance from the State or private companies. I argue that this right constitutes a dimension of privacy. We will see why and how data protection rules may today play a decisive role in its protection.

---

3 Manguel, A. (1996). *A History of Reading*. London: HarperCollins, p.21.

4 Senate Permanent Subcommittee on Investigations of the Committee on Government Operations, Vol. 2, 964 (1953) - reference quoted by Ozer, N. A. (American Civil Liberties Union). *Digital Books: A new chapter for reader privacy* (March 2010). Retrieved September, 3rd, 2013 from https://www.aclunc.org/issues/technology/asset_upload_file295_9047.pdf, p.6.

5 Kaminsky, M. (2012). Reading over your shoulder: social readers and privacy law. *Wake Forest Law Review*, p.17.

6 Lichtblau, E. (2005). F.B.I. Using Patriot Act, Demands Library's Records. *The New York Times* (August 26).

2. READING DATA: AN OPEN WINDOW INTO OUR INTELLECTUAL ACTIVITY

Reading data corresponds with a particular expression of our thoughts and their materialisation in real life, in a specific context and at a given point in time. As a result, they are not an exact mirror, but only a blurred reflection of our ideas. While it is true that a fairly clear picture of our inner life may be extracted from this type of data, the knowledge it provides never entirely corresponds to what really happens in our minds. Furthermore, this type of data is a record of behaviour which sometimes corresponds with a rational choice by the reader, but may also depend on his mood and his whim.

The interpretation of reading data is therefore always uncertain; yet such data is in most cases used by public authorities and companies to predict the intentions of a specific reader, to anticipate his thoughts and to assign a profile to him. Depending on the cases, it can be for example a political or consumer profile. The ultimate goal of this data processing is generally the taking of decisions about the reader.

For this reason, the processing of reading data represents a serious risk to the reader's fundamental rights and liberties. There is an increased likelihood that arbitrary and incorrect decisions will be made about him.

A case which occurred in Britain in 2008 gives an insight into the threat we face. After downloading an al-Qaeda training manual from a US government website, a person was suspected of terrorism by the British police. He was then arrested and detained for seven days. Finally, police realised it was an error and apologised: in fact, he was just a student at Nottingham University who needed this document for research into terrorist tactics[7].

Interestingly, American case law provides us with two examples where reading habits and materials have been introduced as evidence to prove intent in criminal trials[8]. In the case of *United States v. Curtin*[9], the defendant was convicted of the felony crimes of travelling across state lines with intent to engage in a sexual act with a minor and using an interstate facility to attempt to persuade a minor to engage in sexual acts. To prove the specific subjective intent these crimes require, the government successfully used as evidence a number of stories describing sexual acts between adults and children. This lawful[10] reading material was contained in the defendant's personal digital assistant

---

7 Curtis, P. & Hodgson, M. (2008). Student researching al-Quaeda tactics held for six days. *The Guardian* (May 24).
Jones, S. (2011). Student in al-Qaeda raid paid £20,000 by police. *The Guardian* (September 14).

8 Richards, N. M. (2008). Intellectual Privacy. *Texas Law Review*, pp.441-442.

9 *United States v. Curtin*, 305. 489F.3d935 (9th Cir. 2007).

10 See Richards, N. M., *op. cit.*, p.442.

when arrested. In another case, *United States v. Brand*[11], the US Court of Appeal for the Second Circuit allowed the introduction of child pornography found on the defendant's computer to show his predisposition to molest children.

3. FROM PRIVATE SPACES IN WHICH TO READ, TO THE «LIQUID SURVEILLANCE»[12] OF READERS

For a long time, people were able to ensure that their right to read alone was respected by carving out for themselves a private space in which to read. Readers' freedom and autonomy were guaranteed by the existence of private spaces where they could isolate themselves, well away from any form of surveillance. With the paper book, the reader could be sure that nobody could intrude into his reading without his consent. He was the only one to know the content of the book he was leafing through or carefully studying.

Now, as the online environment has led to the disappearance of the frontier between private and public spaces, the reader comfortably seated in his armchair is no longer alone; and it becomes almost impossible to select reading material anonymously. In an age of e-books, tablets and e-libraries, digital content publishers and retailers use advances in technology to collect and process very detailed information on our reading activity.

3.1. The right to read alone, as a dimension of privacy

Traditionally, there are several places dedicated to the consultation of books, to reading and to study. We have specific expectations for each of these as regards privacy. Depending on the status of the room or the place where we are, we can be confident of enjoying a certain level of intimacy and anonymity. These well-defined spaces ensure our control of information relating to our intellectual activity. We can choose to share some aspects with those around us, and to keep others secret.

Of all these places, our private library is without doubt the most intimate. In his *History of Reading*, Alberto Manguel recounts his experience as a reader in his father's library, when he was a teenager: *«I had begun to look up in the elephantine Espasa-Calpe Spanish encyclopaedia, the entries that somehow I imagined related to sex (…) I was curled up in one of the big armchairs, engrossed in an article on the devastating effects of gonorrhoea, when my father came in and settled himself at his desk. Far a moment I was terrified that he would notice what it was I was reading, but when I realize that no one (…) could enter my reading-space, could make*

11 *United-States v. Brand*, 467 F.3d 179, 189 (2d Cir. 2006).

12 This expression is used by Lyon, D. & Bauman, Z. (2013) in their book *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

out what I was being lewdly told by the book I held in my hands, and that nothing except my own will could enable anyone else to know. The small miracle was a silent one, known only to myself»[13].

«There was privacy not only in my reading», explains A. Manguel, *«but also in determining what I would read, in choosing my books in those long-vanished bookstores»*[14]. Our local bookseller could certainly form an idea of our literary tastes by keeping an eye on our purchases, and possibly he judged us accordingly. However he always kept this limited information about our intellectual consumption strictly to himself, and if he kept a record of it, it was in his memory alone.

Public libraries also strive for a balance between control of the reader and the protection of privacy. On the one hand, books must be protected from theft and damage; on the other, readers must be able to gain access to books easily, and concentrate on their research without being disturbed. Our libraries are not only public spaces, but also places of silence and concentration.

Historians agree that the existence of private space for reading and study has played an essential part in the development of a free society, and particularly in the emancipation of women and the working class. The possibility of determining your destiny unhindered, and of questioning the established order, can come only from access to knowledge and learning through books.

Martyn Lyons explains the extent to which this quest for knowledge was difficult for self-taught workers: *«Poverty, lack of time and lack of privacy made study impossible for all except the most dedicated. Cramped housing conditions forced many working-class readers to take to the woods and fields»* [15].

On the question of the emancipation of women, it is particularly instructive to make a detour via painting. In the 18th century, the woman reader was a recurrent theme in French painting[16]. Paintings produced by Jean-Honoré Fragonard[17], François Boucher[18], Jean Raoux[19], Alexis Grimou[20] and Jean-François de Troy[21] portray women absorbed in reading. Their posture and attitude evoke the private nature of the spaces

13 Manguel, A. (1996). *A History of Reading*, *op. cit.*, p.13.

14 *Ibid.*

15 Lyons, M., *op. cit.*, p. 339.

16 Parot, J.-F. *La lecture et la recherche de l'intimité*. Retrieved September, 19th , 2013 from http://www.nicolasleflo ch.fr/Vie-Paris/l-intimite-au-18e-siecle-2.html.

17 La liseuse (c. 1770). National Gallery of Art (Washington).

18 Mme de Pompadour (1756). Alte Pinakothek (Munich).

19 La liseuse, (c. 1716) Musée du Louvre (Paris).

20 First half of the 18th century. Musée des Augustins (Toulouse).

21 La Liseuse (1723). Gemäldegalerie (Berlin).

around them. «Domestic Pleasures», a painting by Jean-Siméon Chardin, was entitled «Amusements de la vie privée» in the original French[22]. Standing before each of these works, we feel as we are intruding in a scene that we should not have witnessed. Jean-François Parot considers these paintings of woman readers to be *«a scale by which we can measure the individualisation of leisure during the Age of Enlightenment.»* The theme recurs in *«Woman in Blue reading a Letter»*, painted by Johannes Vermeer in 1663-64. It met with further success, for example in *«Interrupted Reading»* by Jean-Baptiste Corot[23].

In literature, one could cite «My Mother's House» (originally entitled «La Maison de Claudine») in which Colette tells us that she used to go into the garden with certain books by Emile Zola that her mother had carefully kept her from reading[24]. «Manchester Fourteen Miles» by Margaret Penn is another enlightening testimonial. The writer evokes her youth in the Manchester area. Her illiterate Methodist parents were opposed to all reading except of the Bible and books from Sunday school. Through the intervention of the vicar, her parents finally accepted that she might borrow other books from the Co-op library. Her mother still continued, though, to distrust books which she did not read aloud[25].

This example shows how reading aloud could be used as a way of controlling the reader. In the 19th century, it was not unusual in some Catholic families that *«women were forbidden to read the newspaper. More frequently, a male would read it aloud. This was a task which sometimes implied a moral superiority and a duty to select or censor material»*[26].

Silent and solitary reading, on the other hand, confers an incomparable independence of spirit. The reader can absorb the content at his own pace, without any intermediary, without outside control. He can re-read any passages he wants to; and giving free rein to his imagination, he can develop new ideas while comparing his position with that of the author, questioning it, even refuting it.

The unrestricted physical provision of written material is a prerequisite, without which it is difficult to imagine free access to knowledge. However, it is not enough on its own for the development of independent thinking based on ideas contained in the material. The manner as well as the context in which reading and the study of text take place are crucial factors in this.

---

22 (1746). Nationalmuseum (Stockholm).

23 (1865-1870). Art Institute of Chicago.

24 Colette (1922). *La Maison de Claudine*. Paris: J. Ferenczi & fils, see chapter «Ma mère et les livres».

25 Penn, M. (1947). *Manchester Fourteen Miles*. Sussex: Caliban Books.

26 Lyons, M., *op. cit.*, p.320.

3.2. Reading in an age of e-books, tablets and e-libraries

With the emergence of new technologies for information and communication, silent and solitary reading no longer confers the desired autonomy as it did in the past. The frontiers between private and public spaces have disappeared, leaving surveillance which has become «liquid».

Technical advances can be used to penetrate the inner life of readers and to collect information hitherto known to them alone. Digital content publishers and retailers are now able to collect and process information such as: the search terms we use to find books; the amount of time we spend on a given page; what we have read in the past; how we engage with particular works; and when we get bored[27].

An author recounts that he knows with precision the age, the zip codes, gender and other interests of the people who bought his books. *«Now»*, he said, *«you can throw on top of that the fact that a certain number of them quit reading at Page 45»*[28]. Kobo Inc established that the average reader needs just seven hours to read the final book in S. Collins's *«Hunger Games»* trilogy on the e-reader they produce[29]. Companies active in this sector can also monitor where you read your book or newspaper, thanks to the geolocalisation system with which e-readers are generally equipped. And not only that, they even analyse annotations and highlights.

Amazon, leading company in the e-book market, explains on its website that *«the Amazon Kindle and the Kindle Apps provide a very simple mechanism for adding highlights. Every month, Kindle customers highlight millions of book passages that are meaningful to them. We combine the highlights of all Kindle customers and identify the passages with the most highlights»*[30]. This way, Amazon knows that the two *«most highlighted book of all time»* are the Bible and just after that W. Isaacson's book about Steve Jobs.

The Kobo e-reader's homepage presents *«a dashboard for your literary life»* that is *«a comprehensive overview of all your key reading related activities; your recent reads, personalized recommendations, and Featured Collections all live in one dynamic view»*[31].

---

27 Alter, A. (2012). Your E-Book Is Reading You. *The Wall Street Journal* (July 19).
Kaste, M. (2010). Is Your E-Book Reading Up On You? Retrieved October, 4th, 2013 from http://www.npr.org/2010/12/15/132058735/is-your-e-book-reading-up-on-you.
Glandville, J. (2012). Readers' privacy is under threat in the digital age. *The Guardian* (August 31).

28 Kaste, M. *Ibid.*

29 Alter, A. *Idem.*

30 Retrieved March, 5th, 2014 from https://kindle.amazon.com/most_popular.

31 Retrieved March, 5th, 2014 from http://www.kobo.com/koboarc7hd#readinglife.

In March 2013, Amazon bought Goodreads, a social media site launched in 2007 the aim of which is *«to help people find and share books they love»*[32]. Its 16 million members can add books to their personal bookshelves, see what their friends are reading, add a comment on friends' pages and get suggestions for future reading choices[33].

With social networking we are witnesses to a frenetic exchange and collection of data about intellectual consumption. Trove[34], an application for mobile devices developed by The Graham Holdings Company, is a perfect illustration[35]. Thanks to it, *«you can easily see stories picked by your friends or people you follow»* and get suggestions for contents *«that might interest you based on links you've shared and other Facebook or Twitter activity»*[36].

4. READING, INTELLECTUAL FREEDOM & CREATIVITY

There is a complex relationship between the right to read alone and freedom of expression, including the right to receive information and freedom of thought. In this section of the study, I will demonstrate the close interdependence of these fundamental rights, and conclude that the protection of readers has an impact not only on the ability to exchange information in a society, but also on our intellectual freedom and creativity.

4.1. Role of the reader in the communication process

According to article 10 of the European Convention on Human Rights[37], *«everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas».* From the wording of this provision, the rights to communicate and receive information appear as two inseparable aspects of the same freedom. The judgments of the European Court of Human Rights frequently refer to the importance of these two aspects.[38]

Freedom of expression must be viewed as part of the process of communication between the *transmitter* and the *receiver*. The protection of the *transmitter*, in other words

32 Retrieved March, 5th, 2014 from http://www.goodreads.com/about/us.

33 Retrieved March, 5th, 2014 from http://en.wikipedia.org/wiki/Goodreads.

34 This application was formerly known as the Washington Post Social Reader.

35 See www.trove.com.

36 Retrieved March, 5th, 2014 from http://info.trove.com/faq.

37 signed in Rome by the Member States of the Council of Europe on 4 November 1950.

38 ECHR, *Sunday Times (No. 1) v. the United Kingdom*, judgment of 26 April 1979, §65. See also case of *Lingens v. Austria,* judgement of 8 July 1986, §41 (All the case-law is available at the Court website, at *http://cmiskp.echr.coe.int*).

the person who expresses the idea, has aroused a good deal of interest in legal circles. On the other hand, the liberty of the *receiver* appears to be a question largely ignored. The reason for this situation is that national authorities have for a very long time limited access to information by means of action almost exclusively against the *transmitter*. However, as we know, control will focus more and more directly on the *receiver*. Therefore, it is essential to examine the mechanisms for the protection of the fundamental rights of this vital player in the communication process.

In the exchange of written information, this *receiver* is simply the reader. As Michel de Certeau emphasises, *« the text has a meaning only through its readers»*[39]. In the same sense, Guglielmo Cavallo and Roger Chartier remind us that *«no text exists outside of the physical framework that offers it for reading (or hearing) or outside of the circumstance in which it is read (or heard)»*[40]. In other words, no written communication has any effect without a reader.

The right to read alone allows an idea expressed in writing to reach its public. To this end, it ensures that conditions exist which guarantee both access and the ability to assimilate this information freely. In other words, it facilitates the right to receive information.

Moreover, reading is an intellectual activity. Accordingly, it occupies a privileged position alongside freedom of thought, which is itself at the heart of the concept of the freedom of expression. However the reader cannot develop independent thinking through the study of written works unless he is guaranteed effective protection of his privacy and his personal data. This is precisely what Michael Chabon highlighted in his novel *The Yiddish Policemen's Union*, when he wrote that: *«If there is no privacy of thought –which includes implicitly the right to read what one wants, without the approval, consent or knowledge of others– then there is no privacy, period»*[41].

Based on all this, one can formulate this proposition: The protection of privacy and personal data –including the right to read alone– would appear to be a precondition for the effective exercise of freedom of thought and freedom of expression.

4.2. Readers' freedom and creativity

Reading books, articles and newspapers stimulates our thinking and our imagination, such that new ideas and opinions can emerge. In some cases, these new ideas may

39 de Certeau, M. (1990 – 1st ed. 1980). *L'invention du quotidien - Vol.1: Arts de faire.* Paris: Gallimard, p.251.

40 Cavallo, G. & Chartier, R. (1999). Histoire de la lecture dans le monde occidental. Paris: Editions du Seuil, p.5 (Introduction).

41 Chabon, M. (2007). *The Yiddish Policemen's Union.* New York: HarperCollins.

lead to the creation of original written works, whether in the fields of literature, science or art.

It seems to be universally accepted that creation *ex nihilo* (out of nothing) does not exist. In reality, every creative spirit is inspired by things he already knows or experiences he has already had. The works of the past have always fostered the thinking of authors. From this point of view, free exchange of and access to ample information contributes to the development of a fertile creativity. This allows us to appreciate the impact of reading –and the right to read alone– on creativity.

Furthermore, the conception of a new work also depends on the possibility of withdrawing into solitude, into silence, into a space sheltered from the gaze of others. It was precisely this conclusion that Virginia Woolf reached in *A Room of One's Own* when she wrote that *«A woman must have money and a room of her own if she is to write»*[42]. She considers that *«five hundred a year stands for the power to contemplate»* and that *«a lock on the door means the power to think for oneself »*[43].

The words of John Clare also make it possible to examine the relationship between privacy and creativity. This English 19th century poet, who came from the working class, explained that he *«worked outdoors, composing his work secretly in the fields. He would hide behind hedges and dykes, to scribble down his thoughts on the crown of his hat »*[44].

Finally, the communication to the public of new ideas or new works can be encouraged by some degree of anonymity for the writer. The use of pen names is widespread in the world of literature, as is the use of pseudonyms on the Internet[45].

4.3. How readers' surveillance by companies puts intellectual freedom and creativity in danger

Let's return now to the use made by digital publishers and retailers of data about reading. We still have to identify the purposes of data processing operations carried out by such businesses. In other words, the question is: What is this data for? We are going to show how the pursuit of these aims puts at risk not only the privacy of readers, their right to the protection of personal data, and in particular their right to read alone; but also the two components of their freedom of expression, which are the right to communicate and the right to receive information.

---

42 Woolf., V. (2004 - 1st ed. 1928). *A Room of One's Own.* London: Penguin Books, p.4.

43 *Idem,* p.123.

44 Clare, J. (1951). *The Autobiography: 1793-1824.* In Tibble J.W. & Tibble, A. (eds) *The Prose of John Clare*. London : Routledge & Kegan Paul, p.32.

45 See: Council of Europe. Declaration on Freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies.

Online bookstores pretend to know us better than we know ourselves: they anticipate our wants before we even have time to formulate them. The books you are offered have been automatically selected for you, on the basis of your reading data and in particular of your search history and past purchases. This is from kobo.com: *«Get more of what you love. Kobo Picks analyzes your reading activity and feedback and sends you recommendations based on your personal interests»*[46].

In this case, reading data are processed for the purpose of making individualised contact with consumers so as to offer to sell them products adapted to their purchasing habits. This purpose shows the intrusion of one-to-one marketing into our daily lives.

The personalised bookshop has a serious risk: our choice of written content no longer depends upon our free will. Quite the contrary, it is guided by economic considerations or even the opinions of businesses in the publishing industry. We have therefore abandoned, although we may not realise it, part of our intellectual liberty.

The risk we run is even greater because online bookstores are in no sense sheltered from censorship. It is no longer necessary, as in the past, to withdraw certain works from the shelves or to destroy them. It is enough to simply remove them from the catalogue, so that they still exist but can't be found. In 2009 the de-ranking of gay literature on the Amazon sales site made a lot of waves. Tens of thousands of adult gay and lesbian titles simply disappeared from the ranking system in an attempt to make the *«bestseller lists more family friendly»*[47].

A bookshop which is personalised on the basis of our previous purchases directs us into a deepening groove. One-to-one marketing confines our choices as readers to fixed profiles, when the selection of reading material ought to enable us to develop by discovering new ideas and by contact with opinions different from our own.

Readers' data is also used to produce tailor-made content which matches our expectations. As is often the case, the initial intention seems praiseworthy. *«Better understanding when people stop reading or stop engaging with your content would help you create better products»*[48], explains a publishing consultant. The following sentence, taken from the website of a company specialising in the automatic production of content, could not be clearer about its purpose: «*Imagine creating multiple versions of the same story, with*

46 Retrieved March, 5th, 2014 from http://www.kobo.com/koboaura#readinglife.

47 Flood, A. (2009). Amazon apologises for 'ham-fisted' error that made gay books 'disappear'. *The Guardian* (April 14).
See also: Ashlyn D (2009). *Why We're Not Buying Amazon's Gay Book 'Glitch'*. Retrieved April, 3rd, 2014 from http://www.queerty.com/amazon-says-sorry-for-delisting-gay-books-twitter-doesnt-care-20090413.

48 Kaste, M. (2010). *Cfr. supra.*

each story's content customized for different audiences and tailored to fit a particular voice, style and tone.»[49]

This sort of personalisation of content carries with it, however, an increased risk of conformity and cultural impoverishment. The goal here is to appeal to clearly-identified readers and to produce content which fits in with their ideas. In this universe dominated by marketing, there seems to be little place for the development of original ideas and opposing opinions.

5. DATA PROTECTION MECHANISMS TO ENSURE READERS' FREEDOM

The aim of the right to the protection of personal data is to give individuals control over information related to them, processed by public authorities and businesses. In this section, we shall see how the legal mechanisms put in place to achieve this purpose enable readers to take back control of their data in the digital environment, just as in the world of paper books and physical libraries.

In the European Union, the processing of personal data is mainly regulated by Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter «Directive 95/46/EC»). This text is under revision, since the European Commission has drafted a Regulation proposal 2012/11 (COD) on 25 January 2012[50]. The legislative procedure is still ongoing. Note that the basic principles contained in this directive may also be found in Convention no. 108, adopted by the Council of Europe on 28 January 1981[51]. A reform of this instrument is also under way[52].

Undoubtedly, the purpose principle constitutes one of the most crucial data protection mechanisms. Directive 95/46/EC puts it as follows: «*personal data must be collected for specified, explicit and legitimate purposes*»[53]. This principle permits us to delimit the power of the company or public authority responsible for the processing. The various operations performed on the data must fit within the framework of the purposes

49 See Narrative Science's website. Retrieved January, 29th, 2013 from http://www.narrativescience.com/services.

50 Hereinafter the «Regulation proposal».

51 Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe on 28 January 1981 (hereinafter «Convention n°108»).

52 Modernisation proposals adopted by the 29th Plenary meeting, 27-30 November 2012 (T-PD(2012)4Rev3).

53 Article 6, 1°, b) Directive 95/46/EC. See article 5, b) Regulation proposal ; and also art 5, b) Convention n°108.

defined. This principle enables one to re-establish in the digital world those frontiers which delimited the various spaces for reading that I mention above. Data processing confined by precise purposes comes to replace these spaces.

Of course, it is not possible to analyse in this article all the purposes cited by players in the public and private sectors as reasons for processing personal data about reading. Each relevant data protection principle should be examined separately for each purpose that is envisaged.

As for businesses which operate in the electronic book sector, we have already mentioned the following purposes: (a) the personalised selection of written content offered for sale, in line with the reader's profile; (b) the creation of written content that is personalised with the targeted readership. For the rest of this study, I will focus my analysis solely on these two purposes.

Let's turn to the principle of proportionality set out in article 6(c) of Directive 95/46/EC, according to which the data must be *«adequate, relevant and not excessive in relation to the purposes for which they are collected and / or further processed»*[54]. Regulation proposal 2012/11 (COD) goes much further in its requirements by including the obligation of data minimisation[55] in the formulation of the principle of proportionality. Its article 5(c) states that the personal data must be *«adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data»*.

In practice, the principle of proportionality is implemented by balancing the relevant interests: on the one hand, the privacy of readers; on the other the desire of digital content publishers and retailers to identify the preferences of their public. In the quest for balance, it is appropriate also to take into account the impact on other fundamental rights of the purpose pursued, in this case the freedom of expression and its constituent parts.

On this basis, the processing of data which has anything to do with political, philosophic or religious opinions should be forbidden and considered a breach of the principle of proportionality, even if the reader has consented to the processing of such data. When collecting information about reading, it is difficult to see how businesses operating online bookshops can be sure that they never hold this sort of data about readers. In general, the bulk collection of reading data carried out by businesses in the electronic book sector appears to be inconsistent with the principle of data minimisation.

54 See article 5, c) Convention n°108.

55 This principle has already been highlighted in the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution), adopted at the International Conference of Data Protection and Privacy Commissioners, on 5th November 2009.

Moreover, the consent of readers should be obtained prior to any processing of their data for the two purposes mentioned above, in accordance with article 7 of the Directive[56]. It is prudent to ensure that this consent is specific, as required by article 2(h)[57]. In practical terms, consent with regard to these data purposes should be obtained separately to the customer's acceptance of the contract for sale of books. The reader should be able to buy books in online bookstores, and take advantage of services offered, but still be able to refuse to have his personal data processed for the two above mentioned purposes.

To be effective, consent must also be informed[58]. However, what emerges from an analysis of the standard conditions of the online bookstores most used by European consumers is a lack of transparency. It is very difficult (if not impossible) to establish exactly what data is collected or what use is made of it.

Digital publishers and retailers are generally located in the United States of America; and it is therefore questionable to what extent the current European data protection legislation is and should be applicable when such companies process data related to European readers. Could this contribute to explaining the rather poor level of privacy protection we can observe at the moment in the e-book sector? If so, article 3, §2 of the Regulation proposal 2012/11 (COD) provides an adequate solution. This provision sets the conditions under which the Regulation applies to a controller not established on the European Union territory. The Regulation applies if the processing activities are related to the offering of goods or services to data subjects residing in the European Union, or the monitoring of their behaviour.

In this regard, the Regulation proposal improves the current legislation significantly. Indeed, the national provisions adopted pursuant to Directive 95/46/EC can only be applicable if such a controller makes use of equipment, automated or otherwise, situated on the territory of a member State, and unless such equipment is used only for purposes of transit through the European Union territory[59].

Furthermore, the obligation to process accurate data[60] should contribute to a particularly effective protection for readers. This applies equally to processing carried out by businesses and by public authorities, for whatever purpose it is being done. In fact, we have seen that reading data must in most cases be subjected to interpretation before it yields any really useful data (preferences, opinions, interests, intentions).

56 See article 6, c) Regulation proposal.

57 See article 4, (8) Regulation proposal.

58 Article 2, h) Directive 95/46/EC.

59 Article 4, §1, c) Directive 95/46/EC.

60 article 6, d) Directive 95/46/EC. See: article 5, d) Regulation proposal ; article 5, d) Convention n°108.

And we know that information produced by interpretation of reading data has a very low level of reliability. In the case of a reader who is a natural person, this information is personal data within the meaning of directive 95/46/EC. Therefore it must be accurate.

Of particular interest is also the article 20 of the Regulation proposal, which deals specifically with profiling. Its first paragraph enshrines the right, for every natural person, *«not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour».*

The second paragraph states that, *«subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract (…); or (b)is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent».*

This provision, although innovative, can be criticised on a number of points. The first relates to the methodology used. Before considering the right not to be subject to a measure based on profiling, it appears more logical to set out the conditions under which profiling is authorised. We can also regret the imprecision of the terms «significantly affects», «to evaluate certain personal aspects» and «personal preference» [61]. This lack of clarity may present difficulties when it comes to apply this text. Furthermore, it is unfortunate that this provision does not cover partly automated processing methods[62].

Several lines of thought may be suggested in order to improve this provision. There is no doubt that the creation of profiles raises fundamental rights concerns, as profiles are used to take decisions that may affect individuals whose data are processed. Nevertheless, when seeking adequate protection mechanisms, decision making should be considered separately from the creation of profiles. These two aspects should be understood as distinct parts of a single process.

Following on from this, it becomes clear that the manual, automated or partially automated character of the processing concerns the decision making aspect, and not the elaboration of profiles per se. Moreover, I think that specific rules should be applicable to profiling mechanisms.

---

61 See : Article 29 Working Party. Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012.

62 *Ibid.*

In this research, we have already observed that sensitive data may be used to build profiles which do not concern important aspects of our identity, and on the other hand, that apparently innocuous data may be processed to create highly sensible profiles (for example, related to political opinions).

Article 20, §3 of the Regulation proposal does not take in account this reality. It stipulates that «*automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9*», in other words on sensitive data. Note the use of the expression «solely», which reduces considerably the scope of this provision.

In my opinion, the regime applicable to the processing of sensitive data[63] should provide a satisfactory response to the question of processing sensitive data in order to create a profile. It may also be opportune to consider data related to intellectual activity and consumption (such as data about reading) as new category of sensitive data, and to protect it as such.

Profiles should be considered as sensitive when they formulate a judgement about individuals or label them as regards their opinions, health, sexual orientation or other sensitive aspects.

In order to avoid the creation of profiles inconsistent with the information processed or arbitrary judgments being made about the individual concerned, two requirements should be respected: (a) the category of data processed to establish a profile should be reliable; (b) there should be a logical relationship between the data (or set of data) processed, and the information or knowledge that the profile claims to reveal about the individual.

6. CONCLUSION

Digitalisation of the world of books can be a source of considerable progress, giving easier and faster access to an almost unlimited amount of written material. On the other hand it can also lead to increased monitoring of readers to the point where it threatens free access to information, the possibility of developing independent thought, and creativity.

The use of new technologies for information and communication will not sit well with the development of democracy unless two conditions are met. First, the fundamental rights and liberties of readers online must be given at least as much respect as they are in the world of paper books and physical bookshops. Second, technical progress should be for the benefit of the greatest number, and not only be for the benefit of public authorities and a few businesses.

63 Article 8, Directive 95/46/EC ; article 9 Regulation proposal.

The mechanisms applicable to the protection of personal data can help ensure that these two conditions are met. They guarantee the right to read alone, while giving readers control over their personal data, in an environment where the frontiers between reading spaces have disappeared.

7. BIBLIOGRAPHY

Alter, A. (2012). Your E-Book Is Reading You. *The Wall Street Journal* (July 19).

American Library Association (2005). *Resolution on the USA Patriot Act and Libraries*. Retrieved September, 3rd, 2013 from http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11891.

American Library Association. *The USA Patriot Act*. Retrieved September, 3rd, 2013 from http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact.

Ashlyn D (2009). *Why We're Not Buying Amazon's Gay Book 'Glitch'*. Retrieved April, 3rd, 2014 from http://www.queerty.com/amazon-says-sorry-for-delisting-gay-books-twitter-doesnt-care-20090413.

Cavallo G. & Chartier R. (1999). Histoire de la lecture dans le monde occidental. Paris: Editions du Seuil, p.5.

Chabon, M. (2007), *The Yiddish Policemen's Union.* New York: HarperCollins.

Clare, J. (1951). *The Autobiography: 1793-1824.* In Tibble J.W. & Tibble, A. (eds) *The Prose of John Clare*. London : Routledge & Kegan Paul, p.32.

Colette (1922). *La Maison de Claudine*. Paris: J. Ferenczi & fils.

Curtis, P. & Hodgson, M. (2008). Student researching al-Quaeda tactics held for six days. *The Guardian* (May 24).

de Certeau, M. (1990 – 1st ed. 1980). *L'invention du quotidien - Vol.1: Arts de faire.* Paris: Gallimard, p.251.

Flood, A. (2009). Amazon apologises for 'ham-fisted' error that made gay books 'disappear'. *The Guardian* (April 14).

G. Duhamel (1937). *Défense des Lettres*. Paris: Mercure de France.

Ginzburg, C. (1980). *The Cheese and the Worms - The Cosmos of a Sixteenth-Century Miller*. Baltimore : The Johns Hopkins University Press. Originally published in Italian as *Il formaggio e i vermi : Il cosmo di un mugnaio del'500* (1976).

Glandville, J. (2012). Readers' privacy is under threat in the digital age. *The Guardian* (August 31).

Jones, S. (2011). Student in al-Qaeda raid paid £20,000 by police. *The Guardian* (September 14).

Kaminsky, M. (2012). Reading over your shoulder: social readers and privacy law. *Wake Forest Law Review*, p.17.

Kaste, M. (2010). Is Your E-Book Reading Up On You? Retrieved October, 4th, 2013 from http://www.npr.org/2010/12/15/132058735/is-your-e-book-reading-up-on-you.

Lichtblau, E. (2005). F.B.I., Using Patriot Act, Demands Library's Records. *The New York Times* (August 26).

Lyons, M. (1999). *New Readers in the Nineteenth Century : Women, Children, Workers.* In Cavallo, G. & Chartier (dir.), R. *A History of Reading in the West.* Amherts: University of Massachusetts Press, p.313.

Manguel, A. (1996). *A History of Reading*. London: HarperCollins, p.21.

Ozer, N. A. (American Civil Liberties Union). *Digital Books: A new chapter for reader privacy* (March 2010). Retrieved September, 3rd, 2013 from https://www.aclunc.org/issues/technology/asset_upload_file295_9047.pdf, p.6.

Parot, J.-F. *La lecture et la recherche de l'intimité*. Retrieved September, 19th, 2013 from http://www.nicolaslefloch.fr/Vie-Paris/l-intimite-au-18e-siecle-2.html.

Penn, M. (1947). *Manchester Fourteen Miles*. Sussex: Caliban Books.

Richards, N. M. (2008). Intellectual Privacy. *Texas Law Review*, pp.441-442.

Woolf, V. (2004 - 1st ed. 1928) *A Room of One's Own.* London: Penguin Books.

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y DEFENSA DE LOS CONSUMIDORES

CONTRATACIÓN ELECTRÓNICA CON CONSUMIDORES. TRANSPOSICIÓN AL ORDENAMIENTO JURÍDICO ESPAÑOL DE LA DIRECTIVA 2011/83/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

María Dolores Palacios González
Profesora Titular de Derecho Civil de la Universidad de Oviedo

RESUMEN: La reciente modificación del Real Decreto Legislativo 1/2007 de 16 de noviembre, operada por la Ley 3/2014 de 27 de marzo con el fin de integrar la Directiva 2011/83/UE en el ordenamiento jurídico español, en lo que se refiere a la contratación electrónica con consumidores introduce sobre todo modificaciones en cuanto a requisitos de información al consumidor, a su derecho a desistir del contrato y a las obligaciones de entrega del comerciante. Sin perjuicio de alguna mejora en el Derecho español como ciertas simplificaciones normativas o la determinación de las consecuencias jurídico privadas del incumplimiento de las obligaciones de información del empresario, la conclusión más general que puede extraerse, tanto en relación con la Directiva como con la reforma es que, si bien se produce un avance en la armonización normativa de los Estados de la UE –en su mayor parte es una Directiva de armonización plena– no parece que vaya a ser determinante para el incremento de la contratación por medio de Internet, ni nacional ni transfronteriza. Esto es algo que probablemente depende más de otros factores de carácter sociológico como que las personas nacidas ya en la era tecnológica y del conocimiento de otros idiomas vayan haciéndose adultas y pasen a ser operadores económicos.

PALABRAS CLAVE: Consumidores; comunicaciones comerciales por vía electrónica; contratos a distancia; contratos electrónicos.

1. CONTRATACIÓN ELECTRÓNICA

La Ley 34/2002 de servicios de la sociedad de la información y comercio electrónico (LSSICE) deja bien clara la validez y eficacia de los contratos celebrados por vía electrónica sin necesidad de acuerdo previo de las partes (art. 23). Por tanto, producen todos los efectos previstos por el ordenamiento siempre y cuando, evidentemente, se cumplan los requisitos establecidos en el artículo 1261 del Código Civil. También recoge unas previsiones mínimas relativas a la problemática específica que plantea el soporte que se utiliza para la realización del contrato, sobre todo a efectos de prueba, a la determinación del lugar de celebración del negocio tanto en caso de contratos con consumidores –se presumirán celebrados en el lugar en que el consumidor tenga su

residencia habitual– como entre empresarios o profesionales –en defecto de pacto en el lugar en que esté establecido el prestador de servicios– y a una serie de obligaciones adicionales previas al inicio del procedimiento de contratación y posteriores a la celebración del acuerdo. En todo lo demás la Ley se remite a lo dispuesto en los Códigos Civil y de Comercio, según el caso, y a las restantes normas civiles o mercantiles sobre contratos, en especial las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

Por lo que se refiere a la contratación electrónica con consumidores, en el momento actual esa normativa a que se refiere la Ley se encuentra recogida fundamentalmente en el Real Decreto Legislativo 1/2007 de 16 de noviembre por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU) y, caso de contratos con condiciones generales, como será la mayoría, con carácter general en la Ley 7/1998 de 13 de abril de Condiciones Generales de la Contratación (LCGC).

1.1. El presente de la contratación electrónica con consumidores

La Directiva de 25 de octubre de 2011 del Parlamento Europeo y del Consejo sobre los derechos de los consumidores (2011/83/UE) tiene, entre otras finalidades confesadas, las de simplificar y actualizar las normas aplicables en materia de contratación a distancia y fuera de los establecimientos mercantiles, equilibrar un elevado nivel de protección de los consumidores y la competitividad de las empresas, e incrementar la contratación por medio de la red para aprovechar el potencial de las ventas a distancia transfronterizas que a juicio del legislador comunitario debería de constituir uno de los principales resultados tangibles del mercado interior. Su artículo 4 establece, optando por la armonización plena, que los Estados miembros no mantendrán o introducirán en su legislación nacional disposiciones contrarias a las fijadas en la Directiva, en particular disposiciones más o menos estrictas para garantizar un diferente nivel de protección a los consumidores. Pero se trata de una armonización plena llamada «selectiva» en cuanto se limita a aspectos concretos de la regulación[1].

Como consecuencia del cambio legislativo que impone la Directiva, la Ley 3/2014 de 27 de marzo ha reformado tanto el TRLGDCU como la Ley 7/1996 de Ley de Ordenación del Comercio Minorista (LOCM), cuyos artículos 39 a 48 se derogan de manera que la regulación específica de las ventas a distancia pasa a desarrollarse exclusivamente en el primero. También se modifica la LCGC, precisamente en lo que se refiere específicamente a la contratación electrónica –y también a la telefónica–, quedando sin vigencia el artículo 5.4 que en relación con los requisitos de incorporación de las condiciones

1 Valpuesta Gastaminza, E. (2013). *La propuesta normativa común de compraventa europea. Cuadernos de derecho transnacional*, 5(1), p. 2016.

generales a su vez remitía al Real Decreto 1906/1999, también derogado. Una primera conclusión que se puede extraer es que se avanza por el camino de la simplificación normativa en beneficio de la eficacia y la seguridad jurídicas.

1.2. Contratación a distancia y consumidores

El artículo 92 TRLGDCU define los contratos a distancia como los celebrados en el marco de un sistema organizado de venta o prestación de servicios a distancia, sin la presencia física simultánea del empresario y del consumidor y usuario, y en el que se hayan utilizado exclusivamente una o más técnicas de comunicación a distancia –a la contratación por medio de Internet como técnica de comunicación a distancia se refiere ahora, expresamente, la Ley– hasta el momento de la celebración del contrato y en la propia celebración del mismo. Se suprime la referencia que hacía la redacción anterior a que el sistema de comunicación a distancia estuviese organizado por el empresario, deduciéndose de lo que se explica en la exposición de motivos de la Ley 3/2014 que de lo que se trata es de incluir la contratación por medio de sistemas ofrecidos por un tercero distinto del empresario pero utilizados por éste, como una plataforma en línea. Quedan fuera, sin embargo, los supuestos en que las páginas web ofrecen solamente información sobre el empresario, sus bienes o servicios y sus datos de contacto. En todo caso hay que tener en cuenta que, tras la reforma, a las exclusiones previstas en el TRLGDCU (art. 93) se han añadido otras nuevas si bien en algún caso no es presumible que se concluyan electrónicamente.

La posibilidad de que el empresario utilice técnicas de comunicación a distancia cuyo titular sea otra persona explica que la misma venga también obligada a procurar, en la medida de sus posibilidades y con la diligencia debida, que los empresarios respeten los derechos de los consumidores y cumplan las obligaciones que se les imponen. Lógicamente se excepcionan los prestadores de servicios de intermediación de la sociedad de la información, cuya intervención, por definición neutra y meramente y tecnológica, se regirá por lo previsto en la normativa específica sobre servicios de la sociedad de la información.

Como la Directiva incide incluso en la propia definición de consumidor, que en relación con los contratos contemplados en la misma se refiere a toda persona física que actúe con un propósito ajeno a su actividad comercial, empresa, oficio o profesión, la Ley 3/2014 reforma también el concepto que se asumía en el TRLGDCU, aunque manteniendo lo que ya es nuestra tradición de extenderlo a las personas jurídicas. Pero aún se va más allá considerando consumidores a las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial (ej. comunidades de propietarios).

En cuanto al concepto de empresario, el artículo 4 del TR modificado se refiere a toda persona física o jurídica, ya sea privada o pública, que actúe directamente «o a

través de otra persona en su nombre o siguiendo sus instrucciones, con un propósito relacionado con su actividad comercial, empresarial, oficio o profesión», con clara intención de incluir en su ámbito de aplicación los contratos celebrados por los colaboradores del empresario[2].

2. COMUNICACIONES Y PRÁCTICAS COMERCIALES POR VÍA ELECTRÓNICA

La LSSICE, ya sabemos que no dirigida específicamente a la protección de los consumidores, prevé en su artículo 20 que las comunicaciones comerciales deben identificarse siempre como tales de manera que en el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra «publicidad» o la abreviatura «publi». También deberá de estar claramente identificada la persona física o jurídica de la que proceden. De todas formas se prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente a no ser que el destinatario las haya solicitado o haya prestado su consentimiento expreso o cuando exista una relación contractual previa, en este caso siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente para lo cual los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos y facilitar información accesible por medios electrónicos sobre dichos procedimientos. Queda también prohibido el envío de comunicaciones comerciales en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en el precepto.

En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, las condiciones de acceso y, en

2 Cfr. Botana García, G. (2004), *Los contratos electrónicos a la espera de una nueva reforma, AC*, tomo 1, La Ley.

su caso, de participación, habrán de ser fácilmente accesibles y expresadas de forma clara e inequívoca.

Por otro lado los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios –ej. cookies–, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto (art. 22 LSSICE). Esta previsión, que resulta ciertamente ambigua, ha sido interpretada por la Agencia Española de Protección de Datos en su Guía sobre el uso de las cookies, de manera acorde con la opinión del Grupo de Trabajo del artículo 29, en el sentido de que el consentimiento podrá obtenerse a través de los parámetros adecuados del navegador siempre que el usuario reciba la información adecuada y suficiente sobre los fines del tratamiento de los datos y sobre cómo revocar el consentimiento para su uso y consiguiente eliminación y que realice una acción expresa para modificar la configuración predeterminada que por defecto rechace la recogida y tratamiento de la información.

Por lo que se refiere ya a la normativa específica de protección de los consumidores, las normas que establece el TRLGDCU en materia de prácticas comerciales –cualquier actuación o comunicación directamente relacionada con la promoción, venta o suministro de bienes o servicios (art. 19.2)– y las que las regulan en materias específicas, incluido el comercio electrónico y la comercialización a distancia de servicios financieros destinados a los consumidores, prevalecerán, en caso de conflicto, sobre la legislación general aplicable a las prácticas comerciales desleales, sin perjuicio de que el incumplimiento de todas esas disposiciones sea considerado en todo caso práctica desleal por engañosa en iguales términos a lo dispuesto en el artículo 19.2 de la Ley 3/1991 de 10 de enero, de Competencia desleal, en relación con las prácticas engañosas reguladas en los artículos 20 a 27 (art. 19.4 TRLGDCU). De esta manera, frente a las mismas podrán ejercitarse las acciones previstas en dicha Ley. Seguidamente el artículo 20 prevé que las prácticas comerciales que, de un modo adecuado al medio de comunicación utilizado, incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, deberán contener, si no se desprende ya claramente del contexto, al menos la siguiente información: a) Nombre, razón social y domicilio completo del empresario responsable de la oferta comercial y, en su caso, nombre, razón social y dirección completa del empresario por cuya cuenta actúa. b) Las características esenciales del bien o servicio de una forma adecuada a su naturaleza y al medio de comunicación utilizado. c) El precio final completo, incluidos los impuestos,

desglosando, en su caso, el importe de los incrementos o descuentos que sean de aplicación a la oferta y los gastos adicionales que se repercutan al consumidor o usuario. En el resto de los casos en que, debido a la naturaleza del bien o servicio, no pueda fijarse con exactitud el precio en la oferta comercial, deberá informarse sobre la base de cálculo que permita al consumidor o usuario comprobar el precio. Igualmente, cuando los gastos adicionales que se repercutan al consumidor o usuario no puedan ser calculados de antemano por razones objetivas, debe informarse del hecho de que existen dichos gastos adicionales y, si se conoce, su importe estimado. d) Los procedimientos de pago, plazos de entrega y ejecución del contrato y el sistema de tratamiento de las reclamaciones, cuando se aparten de las exigencias de la diligencia profesional, entendiendo por tal la definida en el artículo 4.1 de la Ley de Competencia Desleal. e) En su caso, existencia del derecho de desistimiento. También el incumplimiento de estas previsiones del artículo 20 será considerado práctica desleal por engañosa en los términos que establece el artículo 7 de la Ley de Competencia desleal, referido a las omisiones engañosas que afectan a la información necesaria para que el destinatario adopte o pueda adoptar conscientemente una decisión económica. Por su parte los apartados 2 y 3 del artículo 21, modificados, prevén por una parte que si los servicios de información y atención al cliente de una empresa utilizan la vía electrónica para llevar a cabo sus funciones deberá garantizar también una atención personal directa y, por otra, que en todo caso los empresarios han de poner a disposición de los consumidores información sobre la dirección postal, número de teléfono y número de fax o dirección de correo electrónico en la que el consumidor pueda interponer sus quejas y reclamaciones o solicitar información sobre los bienes o servicios ofertados o contratados.

En cuanto a las previsiones específicas para las comunicaciones comerciales a distancia con consumidores el artículo 96 reitera que en todas deberá constar inequívocamente ese carácter comercial. En el marco de una relación preexistente el consumidor tendrá derecho a oponerse a recibir comunicaciones por correo electrónico o medio equivalente debiendo ser informado en cada comunicación de los medios sencillos y gratuitos para oponerse a recibirlas. Cuando se utilicen datos personales obtenidos sin el consentimiento del interesado deberá proporcionársele la información prevista en la Ley 15/1999 de protección de datos ofreciendo la posibilidad de rechazarla.

Ya desde la perspectiva concreta de la contratación el artículo 61 TRLGDCU mantiene el carácter vinculante del contenido de la oferta, promoción o publicidad.

3. REQUISITOS DE INFORMACIÓN PREVIOS A LA CONTRATACIÓN

En la exposición de motivos de la LSSICE se destaca su afán por proteger los intereses de los destinatarios de los servicios de la sociedad de la información de forma que puedan gozar de garantías suficientes como tales así como, concretamente, a la hora de contratar un bien o servicio por Internet, con independencia de que se trate o no de consumidores. Es con esta finalidad que «la Ley impone a los prestadores de servicios la obligación de

facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato». Específicamente cuando la contratación se efectúe con consumidores, «el prestador de servicios deberá, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida» (apartado III Exposición de Motivos LSSICE). Y así, con independencia de los requisitos generales de información que han de proporcionar todos los prestadores de servicios de la sociedad de la información (art. 10 LSSICE), el artículo 27 exige que el que realice actividades de contratación electrónica ponga a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los distintos trámites que deben seguirse para celebrar el contrato, si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible, los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y la lengua o lenguas en que podrá formalizarse el contrato. En principio la forma más adecuada al medio de comunicación utilizado parece la utilización de la propia red y, de hecho, la norma entiende que se cumple si el prestador incluye la información en su página o sitio de Internet. Ahora bien, cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario. No hay obligación de facilitar la información si el contrato se celebrada exclusivamente por medio de correo electrónico u otro medio equivalente y en caso de acuerdo entre las partes, pero siempre y cuando ninguna de ellas tenga la consideración de consumidor.

En cuanto a los contratos con condiciones generales, que serán la mayoría, el prestador de servicios deberá ponerlas a disposición del destinatario de manera que éstas puedan ser almacenadas y reproducidas por el mismo (art. 27.4 LSSICE). No sirven, por tanto, las condiciones que se muevan con el cursor, que salgan en una pantalla muy pequeña y que no se puedan imprimir ni grabar. Se trata de una exigencia aplicable a cualquier contrato electrónico, con independencia de la intervención de un consumidor. Con la derogación de los requisitos de incorporación que establecía el RD 1906/1999 para los contratos electrónicos con condiciones generales desaparecen exigencias que en comparación con lo establecido en la LSSICE habían sido calificadas de confusas y excesivas por la doctrina[3].

3 Cavanillas Mújica, S. (2003). *La conclusión del contrato en Internet* en *Responsabilidad civil y contratos en internet*, Granada, Comares, p. 169.

Por su parte la Ley 3/2014 modifica la regulación que, respecto de la información previa a la contratación establecía el artículo 60 TRLGDCU, con carácter general, y el artículo 97 para la contratación a distancia, en particular. A diferencia del régimen superado, que añadía a las exigencias informativas del artículo 97 las generales del 60, en la redacción actual parece que se quieran agotar, en el primer precepto, todos los requisitos de información precontractual que se imponen en la contratación a distancia (y también fuera de establecimientos mercantiles). Son razones que avalan esta apreciación, por un lado que ya no se hace mención a que las obligaciones del articulo 97 son adicionales a las del art. 60 y, por otro, que el artículo 97, en general más completo que el 60, reitera de manera prácticamente idéntica muchas de las previsiones de este último precepto que, por cierto, es el que establece que la información ha de proporcionarse de manera gratuita y al menos en castellano. En cualquier caso, tras la reforma se exige específicamente en el art. 97 para la contratación a distancia y, por tanto, electrónica, que antes de que el consumidor y usuario quede vinculado por el negocio el empresario debe facilitarle de forma clara y comprensible información sobre:

- «Las características principales de los bienes o servicios», si bien «en la medida adecuada al soporte utilizado y a los bienes o servicios».
- La identidad del empresario, incluido su nombre comercial. El artículo 60 incluye la razón social. Además, la dirección completa de su establecimiento, número de teléfono, número de fax y dirección de correo electrónico cuando proceda y también cuando proceda, dirección e identidad del empresario por cuya cuenta actúa. En su caso, y si es diferente, la dirección de la sede del empresario y, cuando proceda, la del empresario por cuya cuenta actúa, a la que el consumidor puede dirigir sus reclamaciones.
- El precio total de los bienes o servicios incluidos impuestos o tasas. Se especifica la información que hay que proporcionar en caso de que por la naturaleza de los bienes o servicios el precio no pueda calcularse razonablemente de antemano o esté sujeto a la elaboración de un presupuesto, en cuyo caso habrá de comunicar la forma en que se determina así como todos los gastos adicionales, de transporte, entrega o postales y cualquier otro gasto –ej. recargos por uso de tarjeta– o, si dichos gastos no pueden ser calculados razonablemente de antemano, el hecho de que puede ser necesario abonarlos. En el artículo 60 se especifica que en el precio total del que siempre hay que informar habrá que desglosar, en su caso, los incrementos o descuentos y todos los gastos adicionales por servicios accesorios, financiación u otras condiciones de pago similares. Por su parte, específicamente para la contratación a distancia el art. 97 e) prevé que en caso de contratos de duración indeterminada o de contratos que incluyan una suscripción, el precio incluirá el total de los costes por periodo de facturación. Cuando se cobren con arreglo a una tarifa fija, el precio total también significará el total de los costes mensuales. Cuando no sea posible calcular razonablemente de antemano el coste total se indicará la forma en que se determina el precio.

- El coste de la utilización de la técnica de comunicación a distancia en caso de que se calcule sobre una base diferente de la tarifa básica.
- Los procedimientos de pago, entrega y ejecución, fecha en que el empresario se compromete a entregar los bienes o ejecutar la prestación y, cuando proceda, el sistema de tratamiento de las reclamaciones del empresario.
- La existencia de garantía legal de conformidad y la existencia y condiciones de los servicios postventa y garantías comerciales. También hay que informar sobre códigos de conducta y la forma de conseguir ejemplares de los mismos, en su caso.
- La lengua o lenguas en que podrá formalizarse el contrato cuando ésta no sea la lengua en la que se ha ofrecido la información previa.
- La duración del contrato o, si es de duración indeterminada o se prolonga automáticamente, las condiciones de resolución. Además, según el 97 q), cuando proceda la duración mínima de las obligaciones del consumidor y usuario derivadas del contrato. Parece referirse a los compromisos de permanencia a los que claramente se refiere el artículo 60 junto con los de vinculación de uso exclusivo de los servicios de un determinado prestador y las penalizaciones en caso de baja.
- La existencia y condiciones del derecho de desistimiento, así como el modelo de formulario de desistimiento. En su caso, la inexistencia del mismo por tratarse de alguno de los supuestos en que así se prevé legalmente. También, cuando proceda, que el consumidor tendrá que asumir el coste de devolución de los bienes y el coste de la misma cuando los bienes no puedan devolverse normalmente por correo. En general, si el consumidor no ha sido adecuadamente informados de la existencia y condiciones del desistimiento, el plazo de 14 días que se tiene inicialmente se amplía a doce meses.
- La existencia y condiciones de los depósitos u otras garantías financieras que el consumidor y usuario tenga que pagar o aportar a solicitud del empresario. Aquí, según la exposición de motivos de la Ley 3/2014, se incluye el importe del bloqueo de tarjetas de crédito o débito.
- En caso de contratos que tengan por objeto contenidos digitales habrá que informar acerca de su funcionalidad, incluidas las medidas técnicas de protección aplicables. El artículo 60 alude, a titulo de ejemplo, a la protección a través de derechos digitales o codificación regional. También sobre toda interoperabilidad relevante del contenido digital con los aparatos y programas conocidos por el empresario o que quepa esperar razonablemente que conozca. También el artículo 60 ejemplifica el sistema operativo, la versión necesaria o determinados elementos de los soportes físicos. Por su parte la exposición de motivos de la ley señala que habrá que describir la información relativa a los aparatos y programas estándar con los que el contenido digital sea compatible.

La obligación de proporcionar información previa a la vinculación contractual se extiende expresamente a los contratos para el suministro de agua, gas o electricidad

cuando no estén envasados para la venta en un volumen delimitado o en cantidades determinadas, calefacción mediante sistemas urbanos y contenido digital que no se preste en un soporte material.

En principio puede entenderse que el requisito de puesta a disposición de la información no exige que necesariamente se haga en la página principal de la web, ni siquiera en páginas de paso obligado, pero en caso de que se trate de información relevante, sobre todo si comporta una obligación para el consumidor –ej. pagos adicionales– sí deberá expresarse en las mismas al menos una mención de que el enlace que lleva a páginas informativas conduce a recibir información en ese sentido[4].

Aunque el artículo 98 TRLGDCU se titula específicamente «requisitos formales de los contratos a distancia» en él se recogen cuestiones que afectan a las obligaciones de información precontractual como la adaptación de la misma a la posibilidad de que se utilicen medios de comunicación con limitaciones técnicas como las pantallas de los móviles que restringen el número de caracteres. En tales casos se prevé un mínimo de información a proporcionar si bien las demás informaciones exigibles según el artículo 97 habrán de facilitarse igualmente de modo apropiado. En definitiva, como señala la exposición de motivos, el consumidor ha de ser remitido a otra fuente de información «por ejemplo facilitando un número de teléfono gratuito o un enlace a una página web del empresario donde la información pertinente esté directamente disponible y sea fácilmente accesible».

Conforme al nuevo artículo 97.8 la carga de la prueba del cumplimiento de los requisitos de información establecidos en este artículo incumbirá al empresario que, si no respeta los referidos a gastos adicionales u otros costes o sobre los costes de devolución de los bienes cuando correspondan al consumidor, se encontrará sin derecho a exigirlos (97.6).

Hasta aquí se observa que pese a la simplificación que supone la unificación de toda la regulación general referida a la contratación a distancia prácticamente se reiteran preceptos (artículos 60 y 97) sin dejar clara la relación entre ambos, aunque la interpretación más lógica sea que el 97 desplaza al 60 que, a su vez, puede complementar al primero. Además, la cantidad de información que el consumidor ha de recibir y el detalle con el que se reglamenta, sobre todo para la contratación electrónica, hacen prever que paradójicamente, por un lado constituya una carga excesiva para el empresario pero, por otro, que se produzca un efecto contrario al garantista deseado.

En cuanto a las contradicciones que puedan producirse con la normativa específica sobre servicios de la sociedad de la información y comercio electrónico, el artículo 94

4 En cuanto a los enlaces se postula que sean visibles, significativos de que se va a proporcionar información y que a cada grupo coherente de información se acceda mediante un enlace diferente Cavanillas Mújica, S. (2003). *La conclusión del contrato en Internet* en *Responsabilidad civil y contratos en internet*, Granada, Comares, p. 176.

TRLGDCU prevé que cuando se den entre lo previsto en el mismo en materia de contratación a distancia y la normativa específica sobre aquellos, esta última será la preferente salvo por lo que se refiere a los requisitos de información precontractual recogidos en el Capítulo I del Título III TRLGDCU que se entenderán como adicionales a los previstos en la Ley 34/2002, pero si una disposición legal o sectorial sobre prestación de servicios, incluidos los de la sociedad de la información y comercio electrónico, relativa al contenido o el modo en que se debe proporcionar la información entrara en conflicto con lo previsto en el Texto refundido, prevalecerá este último (artículo 97.7).

4. FORMACIÓN Y FORMA DEL CONTRATO EN LA CONTRATACIÓN ELECTRÓNICA

Según el artículo 27 LSSICE las ofertas o propuestas de contratación realizadas por vía electrónica, esto es, cualquier comunicación que contenga todos los elementos del contrato proyectado, serán válidas durante el periodo que fije el oferente o, en su defecto, durante el tiempo que permanezcan accesibles a los destinatarios del servicio. Puede plantearse entonces qué ocurre cuando el prestador de servicios no descuelga –revoca– su oferta de la red y el bien o servicio se ha agotado, para concluir que tratándose efectivamente de una oferta, una vez recaída la aceptación la empresa se ve obligada a cumplir o, en última instancia, a responder por el incumplimiento pero, tratándose de contratación electrónica con consumidores, en los términos que veremos posteriormente (arts. 109 ss TRLGDCU).

Para la contratación a distancia con consumidores también se recoge de manera expresa (art. 101 TRLGDCU) que la falta de respuesta a la oferta nunca podrá considerarse como aceptación; se exige aceptación expresa, hasta el punto de que sobre la base de la prohibición de suministrar al consumidor y usuario bienes o servicios no solicitados cuando dichos suministros incluyan una petición de pago de cualquier naturaleza, si igualmente se suministran el receptor no estará obligado ni a su devolución o custodia ni al pago (art. 66 quáter TRLGDCU). Además, en caso de que decida devolverlos no tendrá que indemnizar por los daños o deméritos sufridos por el bien o servicio y a su vez tendrá derecho a ser indemnizado por los gastos y por los daños y perjuicios que se le hubieren causado.

En general y como novedad, para evitar las llamadas «cargas encubiertas» se exige que en todo contrato con consumidores el empresario obtenga su consentimiento expreso para todo pago adicional a la remuneración acordada para la obligación principal. Estos suplementos opcionales han de comunicarse de manera clara y comprensible y su aceptación por el consumidor y usuario ha de realizarse sobre una base de opción de inclusión. Cuando el empresario no obtenga el consentimiento expreso sino que lo deduzca utilizando opciones por defecto que el consumidor tenga que rechazar para evitar el pago adicional, éste tendrá derecho al reembolso (art. 60 bis).

Por su parte el artículo 98 se refiere a los requisitos formales específicos de los contratos a distancia pero en realidad en materia de contratación electrónica pueden reconducirse a la información precontractual, que habrá de proporcionarse al menos en castellano, y a la confirmación de la contratación realizada, a la que aludiremos más adelante. La forma, lógicamente, será la propia del medio de comunicación de manera que en la contratación web la aceptación se realizará mediante el clic correspondiente en condiciones que se manifieste de forma inequívoca la voluntad de contratar. Se realizan al respecto algunas previsiones. El empresario ha de poner en conocimiento del consumidor de manera clara y destacada, justo antes de que efectúe el pedido, la información relativa a características de los bienes, precio total y duración del contrato. Además los sitios web de comercio deberán indicar de modo claro y legible, a más tardar al inicio del procedimiento de compra, si se aplica alguna restricción de entrega y cuáles son las modalidades de pago aceptadas. Cuando el contrato implique obligaciones de pago el empresario deberá velar por que el consumidor y usuario, al efectuar el pedido, confirme expresamente que es consciente de que éste implica dicha obligación. Si la realización de un pedido se hace activando un botón o una función similar, el botón o la función similar deberán etiquetarse, de manera que sea fácilmente legible, únicamente con la expresión «pedido con obligación de pago» o una formulación análoga no ambigua que indique que la realización del pedido implica la obligación de pagar al empresario. El incumplimiento de esta obligación traerá la consecuencia de que el consumidor no quede obligado por el contrato o pedido.

5. LA PRUEBA DEL CONTRATO ELECTRÓNICO

El número 1 del artículo 24 LSSICE remite a las reglas generales del ordenamiento jurídico con la previsión de que si los contratos electrónicos están firmados ha de estarse a lo establecido en el artículo 3 de la Ley 59/2003 de 19 de diciembre, de firma electrónica (LFE) de manera que la firma electrónica reconocida tendrá el mismo valor que la firma manuscrita en relación con el documento en papel. Si no se cumplen los requisitos de la firma electrónica reconocida no por ello carece de efectos jurídicos y, en todo caso, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí se tendrá en cuenta lo estipulado entre ellas (art. 3. 9 y 10 LFE).

El soporte electrónico en que conste un contrato será admisible en juicio como prueba documental (art. 24 LSSICE) con carácter de documento electrónico, que además puede tener la naturaleza de documento público si está firmado electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso (art. 3.6.b) LFE. Si el documento está firmado y se impugnare en juicio la autenticidad de la firma electrónica reconocida se procederá a comprobar que se base en una firma electrónica avanzada basada en un certificado reconocido y que la

firma se ha generado mediante un dispositivo seguro de creación de firma electrónica. La carga de realizar las comprobaciones corresponde a quien haya presentado el documento. Si el resultado es positivo se presume la autenticidad de la firma electrónica reconocida. Si se impugna la autenticidad de la firma electrónica avanzada quien haya presentado el documento podrá proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto. Si no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica (art. 326.2 LECivil).

Además, según prevé el artículo 25 LSSICE las partes pueden pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. El tercero deberá archivarlas por el tiempo estipulado, no inferior a cinco años.

6. CONFIRMACIÓN DE LA CONTRATACIÓN

De acuerdo con el artículo 28 LSSICE en la contratación electrónica– salvo por medio de correo electrónico u otro tipo de comunicación electrónica equivalente cuando no sean empleados con el exclusivo propósito de eludir la obligación - el oferente tiene que confirmar la recepción de la aceptación con el fin de proporcionar al contratante aceptante tanto la prueba de la perfección del contrato como certeza del contenido del mismo. Cabe mediante el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, lo que suele hacerse por medio de un correo electrónico inmediato o, a más tardar una vez que el aceptante haya completado el procedimiento, por un medio equivalente al utilizado en el procedimiento de contratación y que permita que la confirmación sea archivada por el destinatario. Concretamente esto último suele hacerse mediante una última pantalla que sigue a aquella en la que el aceptante accede a finalizar el proceso. En los casos en que la obligación de confirmación corresponda a un destinatario de servicios el prestador ha de facilitar el cumplimiento poniendo a disposición del destinatario alguno de estos medios. La norma prevé también que se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello. Es de destacar que la derogación del RD 1906/1999 y del artículo 47 LOCM que recogían previsiones al respecto simplifica y clarifica el régimen aplicable a la obligación de confirmación de la contratación realizada.

Para los contratos a distancia con consumidores se matiza, en el artículo 98.7 TRLGDCU, que la confirmación habrá de hacerse en soporte duradero[5]. También que

5 El TRLGDCU define, en el art. 59 bis, el «soporte duradero» como todo instrumento que permita al consumidor y usuario y al empresario almacenar información que se le haya dirigido

ha de hacerse en un plazo razonable después de la celebración del contrato y a más tardar en el momento de entrega de los bienes o antes del inicio de la ejecución del servicio. La confirmación ha de incluir toda la información prevista para antes de celebrarse el contrato en su artículo 97.1 salvo que ya se haya facilitado en un soporte duradero. También ha de indicarse, cuando proceda, la confirmación del previo consentimiento expreso del consumidor y del conocimiento por su parte de la pérdida del derecho de desistimiento por tratarse de suministro de contenido digital que no se presta en soporte material si la ejecución ha comenzado con su previo consentimiento expreso y conocimiento de aquella pérdida.

En caso de incumplimiento de la obligación de confirmación el artículo 100 TRLGDCU permite la anulación instancia del consumidor y usuario por vía de acción o excepción. En ningún caso podrá ser invocada la causa de nulidad por el empresario, salvo que el incumplimiento sea exclusivo del consumidor.

7. CONDICIONES DE EJECUCIÓN DEL CONTRATO

Tras la reforma y de acuerdo con la Directiva se regula más ampliamente el derecho de desistimiento en los contratos a distancia y fuera de establecimiento mercantil –salvo las excepciones recogidas en el artículo 103 TRLGDCU– cuyo plazo de amplía de 7 días hábiles a 14 días naturales. Se incorpora además un formulario normalizado que el consumidor podrá utilizar al efecto. Si no se ofrece al consumidor la información exigible sobre este derecho el plazo para desistir se amplía a doce meses. El empresario puede, además, ofrecer la opción de cumplimentar y enviar electrónicamente el modelo de formulario de desistimiento o cualquier otra declaración inequívoca a través del sitio web del empresario. En estos casos el empresario ha de comunicar sin demora, en soporte duradero, el acuse de recibo del desistimiento. En los artículos 107 y 108 TRLGDCU se recogen ahora, detalladamente, los derechos y obligaciones de las partes en caso de desistimiento.

La regla general en contratos de consumo a distancia y, por tanto, en la contratación electrónica es, según el artículo 109 TRLGDCU, que salvo acuerdo entre las partes el empresario deberá ejecutar el pedido a más tardar en el plazo de 30 días –se concreta ahora que naturales– a partir de la celebración del contrato.

---

personalmente de forma que en el futuro pueda consultarla durante un período de tiempo acorde con los fines de dicha información y que permita su fiel reproducción. Entre otros, tiene la consideración de soporte duradero el papel, las memorias USB, los CD-ROM, los DVD, las tarjetas de memoria o los discos duros de ordenador, los correos electrónicos, así como los mensajes SMS.

Se ha modificado la regulación prevista para el caso de no ejecución por parte del empresario por falta de disponibilidad del bien o servicio. Conforme a la nueva reglamentación ha de informar al consumidor y devolverle las sumas abonadas «sin ninguna demora indebida»[6]. Se produce, por tanto, una disminución en su protección ya que antes se recogía un plazo máximo de 30 días y ahora, en definitiva, se deja en manos del empresario el momento de devolución de lo abonado. Sí es cierto que se prevén consecuencias en caso de retraso injustificado, manteniéndose que esta será la devolución del doble de lo adeudado sin perjuicio del derecho del usuario a ser indemnizado por los daños y perjuicios sufridos en lo que excedan de dicha cantidad, pero en la práctica podría no ser fácil determinar la existencia de esa falta de justificación.

Se sigue manteniendo, sin embargo, la previsión de que de no hallarse disponible el bien o servicio contratado cuando el consumidor hubiera sido informado expresamente de tal posibilidad el empresario pueda suministrar sin aumento de precio un bien o servicio de características similares que tenga la misma o superior calidad (art. 111 TRLGDCU).

Por lo que se refiere al pago el consumidor titular de la misma puede exigir la inmediata anulación del abono que se haya cargado a una tarjeta de manera fraudulenta o indebida, debiendo realizarse las anotaciones de adeudo y reabono en las cuentas del empresario y del titular a la mayor brevedad. Lo que ocurre es que en el comercio «on line» si se entiende que la prueba del fraude corresponde al comprador resulta imposible al no existir firma manuscrita. Si, por el contrario, se presume el fraude, la empresa habrá de aceptar todos los rechazos que se le presenten, con la posibilidad de abusos, o bien de establecer sistemas de autenticación de usuarios, con el coste que supone cualquier de las dos opciones[7]. Si la compra hubiese sido efectivamente realizada por el consumidor y usuario y la exigencia de devolución no fuera consecuencia de haberse ejercicio del derecho de desistimiento o resolución, quedará obligado frente al empresario al resarcimiento de los daños y perjuicios causados como consecuencia de la anulación (art. 112.2 TRLGDCU).

Por otro lado, también como en otras previsiones para evitar cargas encubiertas, los empresarios no pueden facturar a los consumidores y usuarios, en ningún contrato de consumo, por el uso de determinados medios de pago, cargos que superen el coste soportado por los mismos por el uso de tales medios.

---

6 Puede discutirse aquí si también son aplicables las especialidades del régimen general recogido en el art. 62 bis) como postula Carrasco Perera, A. (2014). «Entrega de los bienes vendidos, resolución y traslado de los riesgos en la compraventa al consumo», Revista CESCO de Derecho del consumo, http://www.revista.uclm.es/index.php/cesco.

7 Llaneza González, P. (2003), *Aplicación práctica de la LSSI-CE*, Barcelona, p.42.

8. UNA CRÍTICA FINAL

Aunque se haya avanzado algo para simplificar la normativa que regula la contratación electrónica con consumidores aún queda camino por recorrer. De hecho, la transposición de la Directiva se ha llevado a cabo mediante una técnica legislativa discutible, sin cuidar la coherencia interna del Texto Refundido, manteniendo además duplicidades y frecuentes remisiones. Todo ello, al menos en una primera aproximación, lleva más bien a la inseguridad y, por tanto, hace prever una menor eficacia de la deseable.

9. BIBLIOGRAFÍA

Botana García, G. (2014). *Los contratos electrónicos a la espera de una nueva reforma, AC*, tomo 1, La Ley.

Carrasco Perera, A. (2014). «Entrega de los bienes vendidos, resolución y traslado de los riesgos en la compraventa al consumo», Revista CESCO de Derecho del consumo, nº 9/2014, http://www.revista.uclm.es/index.php/cesco.

Cavanillas Mújica, (2003). *La conclusión del contrato en Internet* en *Responsabilidad civil y contratos en internet*, Granada, Comares.

Llaneza González, P. (2003), *Aplicación práctica de la SSI-CE*, Barcelona.

Valpuesta Gastaminza, E. (2013). *La propuesta normativa común de compraventa europea. Cuadernos de derecho transnacional*, 5(1).

Zurilla Cariñana, M.A, (2014). «La reforma de los arts. 60 y 97 de la Ley de modificación del TRLGDCU. ¿Hay alguna novedad que merezca la pena?, Revista CESCO de Derecho del consumo, nº 9/2014, http://www.revista.uclm.es/index.php/cesco.

NOVEDADES DEL DEBER DE INFORMAR AL CONSUMIDOR EN LA CONTRATACIÓN ELECTRÓNICA

María Arias Pou
Directora de ARIAS POU Abogados TIC
Coordinadora de la Comisión de Menores de APEP
Profesora de Derecho de las Nuevas Tecnologías de la Universidad Europea de Madrid

RESUMEN: En la presente comunicación se analizan los cambios normativos que han tenido lugar en relación con el deber de los prestadores de servicios de informar al consumidor en un proceso de contratación electrónica. A través del análisis de las novedades que introduce la nueva Directiva sobre derechos de los consumidores y de la evolución de los distintos textos normativos españoles que se han ido aprobando hasta trasponer esta Directiva a nuestro ordenamiento jurídico interno, analizaré cómo ha variado el contenido de este deber de información tras la última reforma del texto de consumidores.

De este modo, expondré la dispersión normativa a la que debe acudir el prestador de servicios para conocer, en toda su extensión, cuál es el contenido de la información que debe proporcionar al consumidor en un proceso de contratación electrónica, partiendo del hecho de ser esta contratación caracterizada por ser una contratación con consumidores, a distancia y por vía electrónica.

La tímida corrección de la excesiva remisión normativa, incluso en el mismo texto de consumidores, la introducción de la idea de 'información mínima' a proporcionar para adaptarse a las limitaciones como la del número de caracteres en determinadas pantallas de teléfono móvil, a través del que se realiza la contratación o el concepto de soporte duradero, como medio para facilitar la información, son algunas de las principales conclusiones.

PALABRAS CLAVE: Deber de información, contratación electrónica, consumidor, soporte duradero, prestador de servicios de la sociedad de la información.

1. EL DEBER DE INFORMACIÓN EN LA CONTRATACIÓN ELECTRÓNICA

Comenzaré esta comunicación señalando las características del panorama normativo existente en el momento de escribir la misma. Nos encontrábamos de camino hacia la transposición, a nuestro ordenamiento jurídico interno, de la Directiva 2011/83/UE[1], la nueva Directiva de derechos de los consumidores, que otorgó a los Estados miembros

1 Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directi-

un plazo, hasta el 13 de diciembre de 2013, para transponer a su ordenamiento sus nuevas exigencias. Pocos días antes de concluir esta comunicación, el BOE publicaba la Ley 3/2014[2] por la que se modifica el Texto Refundido de Consumidores, por lo que vamos a tratar de analizar esta cuestión a la vista de las recientes novedades que se introducen en el ámbito de la información al consumidor en la contratación electrónica.

Hablar de contrato electrónico con consumidores nos lleva a tener presente la realidad de que este tipo de contratación se enmarca en el ámbito de consumo y de contratación a distancia, por medios electrónicos. De esta forma, la normativa aplicable se encuentra dispersa entre las normas que regulan la contratación con consumidores, la contratación a distancia y la contratación electrónica. Por este motivo, para este análisis abordaremos el régimen comunitario de la Directiva 97/7/CE y el futuro régimen de la Directiva 2011/83/UE[3], y en el ámbito nacional trataremos el Texto Refundido de Consumidores[4], TRLGDCU, y las distintas iniciativas de Anteproyecto y Proyecto de Ley que se han ido aprobando hasta la reciente Ley 3/2014, con el fin de cumplir el mandato de la nueva Directiva sobre derechos de los consumidores y nos referiremos a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico[5], como ley sectorial aplicable.

El deber de informar al consumidor encuentra su base legal, en nuestro ordenamiento, en el artículo 51 de la CE[6] como un principio rector de la política social y económica. Este artículo fue desarrollado por primera vez por la LGDCU[7] y en su re-

va 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. DOUE L. 304, de 22 de noviembre.

2 Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre. BOE núm. 76, de 28 de marzo. A esta Ley le han precedido un Anteproyecto de Ley aprobado el 24 de julio de 2012 por el Ministerio de Sanidad, Servicios Sociales e Igualdad y un Proyecto de Ley publicado en el BOCG, 25 de octubre de 2013, Núm. 71-1, Serie A: Proyectos de Ley 121/000071.

3 Conforme al artículo 28 de la Directiva, las disposiciones de esta norma se aplicarán a los contratos celebrados después del 13 de junio de 2014. Esta misma fecha establece la Disposición transitoria primera de la Ley 3/2014 para su aplicación.

4 Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias. BOE núm. 287, de 30 de noviembre.

5 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE núm.166, de 12 de julio.

6 Constitución Española de 27 de diciembre de 1978. BOE núm. 311, de 29 de diciembre.

7 Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios. BOE núm. 176, de 24 de julio. En adelante, LGDCU.

dacción original, recogía el derecho a la información como uno de los derechos básicos del consumidor a recibir:

> La información correcta sobre los diferentes productos o servicios y la educación y divulgación, para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.[8]

El desarrollo de este derecho a la información, implica, explica Macías Castillo[9]:

> el desarrollo de un principio rector de la política social y económica en nuestro ordenamiento jurídico, como es la protección y defensa de los consumidores y usuarios a través, fundamentalmente, de la articulación de remedios eficaces –judiciales o no–, pero desde luego, también desde la formación y la educación.

Este autor caracteriza la información debida al consumidor como 'instrumental', pues considera que su contenido determinará en buena medida la contratación de un servicio (información precontractual) o el correcto y satisfactorio desarrollo del mismo (información contractual), en el supuesto en el que la perfección del contrato haya tenido lugar. Y añade que también la información cumple un importante papel de cara a la evitación de daños, personales o materiales, en la persona del propio contratante o de terceros ajenos a la relación contractual.

Bercovitz[10] ha escrito que, frente a los derechos del consumidor que califica de fundamentales el derecho del consumidor a la información sería un derecho de carácter instrumental. Por su parte, Gómez Segade[11] matiza que en la Constitución, el derecho a la información del consumidor sólo puede ser aceptado implícitamente, debido a su carácter instrumental, como derivado de los derechos fundamentales del consumidor reconocidos expresamente en el 51.1.

Siguiendo esta doctrina, entendemos que el deber de información persigue así, en primer lugar, ofrecer al consumidor los datos necesarios para permitirle otorgar un consentimiento libre y debidamente formado, derivado de una correcta y completa información sobre el bien o servicio que está interesado en contratar. En segundo lugar, este deber es determinante para que, en el caso de que el consumidor decida contratar, el uso y disfrute del bien o del servicio por el consumidor, se lleve a cabo satisfactoriamente y sin incidentes ocasionados por una falta de información o por una información incompleta.

---

8 Artículo 2.1. d) de la LGDCU.

9 MACÍAS CASTILLO, A. (2005). Comentario al artículo 13 de la LGDCU. En LLAMAS POMBO, E. (Coordinador), Ley General para la Defensa de los Consumidores y Usuarios. Comentarios y Jurisprudencia de la Ley veinte años después. Madrid: La Ley. p. 505.

10 BERCOVITZ, A. y BERCOVITZ, R. (1987) Estudios jurídicos sobre protección de los consumidores. Madrid: Tecnos. p. 26.

11 GÓMEZ SEGADE, J.A. (1980). Notas sobre el derecho de información del consumidor. Revista Jurídica de Cataluña n. 3. p.144.

La necesidad del reconocimiento de este derecho y la importancia que ya la LGDCU le dio lo explica Lasarte Álvarez[12] diciendo que una de las causas fundamentales del debilitamiento del consumidor es la falta de transparencia en el mercado, es decir, la ausencia de una información adecuada y suficiente.

Dicho esto y para terminar de centrar el objeto de este análisis diré que el derecho del consumidor a estar informado, en el ámbito de la contratación electrónica, implica necesariamente un deber del prestador de servicios de informar. Esta idea, que resulta obvia, en ocasiones lleva a error dado que en la normativa que vamos a analizar el legislador utiliza el término de 'derecho' cuando en su contenido está describiendo un 'deber'.

GARCÍA VICENTE[13] lo explica así:

> Cabe advertir que aunque se afirme el «derecho» a la información de los consumidores o usuarios, su desarrollo legal se construye desde los «deberes» (que es un par inescindible), deberes imperativos y predeterminados que pesan sobre el empresario o profesional para satisfacerlo. No obstante, y pese a la declaración de los arts. 8 d) y 17.1 TRLGDCU, «no» hay un derecho del consumidor a solicitar información del empresario o profesional sobre cuantas circunstancias influyan en la celebración y/o ejecución del contrato: este derecho exige la mediación legal.

He creído conveniente terminar esta introducción con esta aclaración, para facilitar la comprensión de lo que en este trabajo nos hemos propuesto abordar: el deber de los prestadores de servicios de informar al consumidor en la contratación electrónica.

2. EL DEBER DE INFORMACIÓN EN LA NORMATIVA COMUNITARIA

La nueva Directiva sobre los Derechos de los consumidores denuncia en su Considerando 5 que no se aprovecha plenamente el potencial de las ventas a distancia transfronterizas, cuando debería constituir uno de los principales resultados tangibles del mercado interior. Y argumenta que, entre los factores que ralentizan el crecimiento del potencial transfronterizo, destacan las diferentes normas nacionales de protección de los consumidores impuestas a las empresas. Por este motivo, la Directiva apuesta porque la plena armonización de determinada información facilitada al consumidor y del derecho de desistimiento en los contratos a distancia y los contratos celebrados fuera del establecimiento contribuirá a un elevado nivel de protección de los consumidores y a un mejor funcionamiento del mercado interior entre empresas y consumidores.

---

12 LASARTE ÁLVAREZ, C. (2007) *Manual sobre protección de consumidores y usuarios* (3ª Ed.). Madrid: Dykinson. p. 105.

13 GARCÍA VICENTE, J.R., (2013). 10. La contratación con consumidores. En BERCOVITZ RODRÍGUEZ CANO, R.,(DIRECTOR), TRATADO DE LOS CONTRATOS. TOMO II (2ª Ed.). Valencia: Tirant lo Blanch. p. 1652.

Para proponer esta Directiva, la Comisión se apoyó en el Libro Verde sobre la revisión del acervo en materia de consumo[14] que describió como objeto global de su revisión instaurar un auténtico mercado interior para los consumidores, estableciendo el equilibrio adecuado entre el alto nivel de protección de éstos y la competitividad de las empresas, al tiempo que se garantiza el estricto respeto del principio de subsidiariedad. Y concluía que lo ideal sería que, al término del ejercicio, fuera posible decir a los consumidores de la UE: «Esté donde esté o compre donde compre en la UE, sus derechos básicos son los mismos».

Guillén Catalán[15], comentando la Directiva, señala:

> En la actualidad existen notables diferencias entre los distintos Estados miembros de la Unión Europea en los necesarios deberes de información que debe contener las ofertas contractuales y las diferentes modalidades de ejercicio del derecho de desistimiento que han ocasionado costes a las empresas que realizan ventas intracomunitarias y generan inseguridad jurídica en los consumidores. Con el objetivo de armonizar los aspectos más básicos de la protección de los consumidores y usuarios en el ámbito de la Unión Europea, se ha aprobado la citada Directiva.

Por su parte, el Considerando 9 prevé el *establecimiento de* normas relativas a la información que es preciso facilitar *en los contratos a distancia y en los contratos celebrados fuera del establecimiento, así como en los contratos distintos a los contratos a distancia y los contratos celebrados fuera del establecimiento.* Además, el Considerando 12 contempla los requisitos de información que establece la Directiva como complementarios de los requisitos de información que establecen Directivas como, a los efectos que nos ocupan en este trabajo, los previstos en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior y mantiene la posibilidad de que los Estados miembros impongan requisitos de información adicionales aplicables a los prestadores de servicios establecidos en su territorio nacional.

Antes de seguir avanzando en el conocimiento del contenido del deber de información en la Directiva, queremos traer a colación la reflexión de Bednarz[16] que dice:

> Asimismo parecen beneficiosas desde el punto de vista de los consumidores, las normas sobre la información precontractual que les deberán facilitar los comerciantes. Claramente no se puede adquirir bienes a través de Internet sin conocer sus principales características. Igualmente la

14 Libro Verde sobre la revisión del acervo en materia de consumo. Presentado por la Comisión Europea el 8 de febrero de 2007, COM(2006) 744 final, Bruselas.

15 GUILLÉN CATALÁN, R. (2012). La Directiva sobre los derechos de los consumidores: un paso hacia delante, pero incompleto. Diario La Ley (Nº 7801, de 20 Febrero de 2012).

16 BEDNARZ, Z., (2012) ¿Cómo influirá la nueva Directiva 2011/83/UE en el comercio electrónico?. En *Actas del VIII Congreso Internacional Internet, Derecho y Política*, celebrado los días 9 y 10 de julio de 2012, Universidad Oberta de Cataluña, p. 179.

información relevante al comerciante parece apropiada. Sin embargo, hay que tener en cuenta que las exigencias sobre información precontractual de la Directiva analizada están completadas por otros actos normativos. Así, surge la pregunta de si el consumidor realmente podrá asimilar tanta cantidad de información.

Esta es a nuestro entender, una de las principales cuestiones en materia de información al consumidor, ¿estamos 'sobreinformando' al consumidor? A través del estudio de las exigencias normativas de información pondré de manifiesto la ingente cantidad de información que están obligados a proporcionar los prestadores de servicios en el ámbito de la contratación electrónica. Y la cuestión que planteamos es si realmente una vez cubiertos todos estos aspectos informativos el consumidor queda realmente informado.

A efectos de analizar los requisitos de información que, en cada caso, prevé la Directiva, queremos destacar la comparativa que Guillén Catalán realiza sobre el artículo 5 que trata de los requisitos de información cuando los contratos no son a distancia ni celebrados fuera del establecimiento mercantil, y los requisitos del 6 que rige para los contratos a distancia y los celebrados fuera del establecimiento.

Vamos a ir analizando, paso a paso, las diferencias entre uno y otro precepto; para ello utilizaremos un análisis comparativo de estos preceptos:

Art. 5 Directiva 2011/83/CE Requisitos de información de los contratos distintos de los contratos a distancia o los celebrados fuera del establecimiento	Art. 6 Directiva 2011/83/CE Requisitos de información de los contratos a distancia y los contratos celebrados fuera del establecimiento
1. Antes de que el consumidor quede vinculado por un contrato distinto de un contrato a distancia o uno celebrado fuera del establecimiento, u oferta correspondiente, el comerciante deberá facilitar de forma clara y comprensible al consumidor, *salvo que dicha información resulte evidente por el contexto*:	1. Antes de que el consumidor quede vinculado por cualquier contrato a distancia o celebrado fuera del establecimiento o cualquier oferta correspondiente, el comerciante le facilitará de forma clara y comprensible la siguiente información:

Si observamos la redacción de estos dos párrafos, destacamos como diferencias, de un lado, que en la contratación 'presencial', el comerciante o empresario, puede verse exceptuado de ofrecer explícitamente determinada información, porque ésta resulte deducible del contexto que rodea la contratación. Condición que el legislador considera que no puede tener lugar en el entorno de la contratación a distancia. Destacar también, como el legislador ha incluido definitivamente como características de esta información y en ambos casos, que sea clara y comprensible, cuestión ésta que resulta necesaria para que el consumidor quede realmente informado al contratar.

En cuanto al contenido de la información, destacamos las diferencias:

- En relación con la identidad y dirección del comerciante, cuando la contratación es a distancia se exige, además de la identidad del comerciante, como su nombre

comercial; y la dirección geográfica del establecimiento del comerciante y el número de teléfono, que se facilite al consumidor el número de fax y dirección de correo electrónico del mismo, cuando proceda, con objeto de que el consumidor pueda ponerse en contacto y comunicarse con él de forma rápida y eficaz así como, cuando proceda, la dirección geográfica y la identidad del comerciante por cuya cuenta actúa.

Entiendo necesario que en la contratación a distancia, el consumidor deba recibir más datos de contacto del empresario, porque así se consigue acortar la distancia entre las partes, y se ofrece una mayor seguridad al consumidor. Destacamos en esta redacción la referencia a que los datos que se ofrecen, permitan al consumidor ponerse en contacto y comunicar con el comerciante, de forma «rápida y eficaz». En el entorno electrónico[17], el legislador también viene exigiendo que los datos de contacto sean suficientes para que la comunicación sea directa y eficaz. La interpretación de esta finalidad ha supuesto algunos conflictos entre las partes interesadas como en el caso[18] de la Federación Alemana de Asociaciones de Consumidores, el Bundesverband, donde consideró que DIV, empresa de seguros y a los efectos que nos interesan, el prestador de servicios, estaba obligada a indicar su número de teléfono en su sitio Internet. Según esta organización, éste era el único modo de garantizar una comunicación directa entre un cliente potencial y dicha compañía de seguros.

En este caso la conclusión del TJUE fue que en virtud del artículo 5.1 c) de la Directiva, el prestador de servicios está obligado a proporcionar a los destinatarios del servicio un medio de comunicación rápido, directo y efectivo, complementario a su dirección de correo electrónico. Pero esto no significa que estas informaciones tienen que incluir necesariamente un número de teléfono, pueden consistir en un formulario de contacto electrónico mediante el cual los destinatarios del servicio puedan dirigirse por Internet al prestador de servicios y al que éste responda por correo electrónico, salvo en las situaciones en las que un destinatario del servicio que, tras la toma de contacto por vía electrónica con el prestador de servicios, se encuentre privado de acceso a la red electrónica solicite a éste el acceso a un medio de comunicación no electrónico.

17 Artículo 5 de la Directiva 2000/31/CE y los artículos 10 y 27 de la LSSI.

18 Sentencia del Tribunal de Justicia (Sala Cuarta) de 16 de octubre de 2008. En el asunto C-298/07, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 234 CE, por el Bundesgerichtshof (Alemania), mediante resolución de 26 de abril de 2007, recibida en el Tribunal de Justicia el 22 de junio de 2007, en el procedimiento entre Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV y Deutsche internet versicherung AG.

- En relación con el precio, es importante resaltar, en este caso, no por diferencia entre la contratación presencial o a distancia sino para que en la práctica se tenga en cuenta, que el precio señalado debe indicar claramente los impuestos, cuestión esta que en el entorno electrónico ha dado numerosos problemas al no detallar esta información y ofrecer al consumidor una información confusa o, al menos, incompleta. BEDNARZ[19] resume así esta información referida al precio:

  > La obligación del empresario de exponer el precio completo significará que el consumidor mientras contrate *on-line*, tendrá que conocer el precio total del bien o servicio antes de hacer un pedido. Es decir, no podrá aparecer ningún coste adicional después de entrar en el formulario de pedido.

Por su parte, si comparamos el artículo 6 de la nueva Directiva con su correspondiente de la Directiva 97/7/CE, el artículo 4, nos encontramos con que para los contratos a distancia, la Directiva 97/7/CE prevé que la información que acabamos de describir, sea facilitada por el comerciante de forma acorde con las técnicas de comunicación a distancia utilizadas y en términos claros y comprensibles. Además, conforme al artículo 5 de la Directiva 97/7/CE, el comerciante deberá facilitar al consumidor la confirmación del contrato celebrado en un soporte duradero[20], que deberá ser legible y en un plazo razonable después de la celebración del contrato, a más tardar en el momento de entrega de los bienes o antes del inicio de la ejecución del servicio. La Directiva 2011/83/UE establece que en dicha confirmación se debe incluir toda la información que figura en el art. 6.1, salvo si el comerciante ya ha facilitado la información al consumidor en un soporte duradero antes de la celebración del contrato a distancia, y en el supuesto expresamente previsto por la Directiva, la confirmación del previo consentimiento expreso del consumidor y del conocimiento por su parte, de la pérdida del derecho de desistimiento.

Cuando el contrato se celebra a través de una técnica de comunicación a distancia en la que, el espacio o el tiempo, para facilitar la información son limitados, por ejemplo, la pantalla de un teléfono móvil, se prevé la obligación del comerciante de facilitar

19 BEDNARZ Z., Ob. cit., p. 174.

20 La Directiva 2011/83/CE define el soporte duradero, artículo 2. 10), como: «todo instrumento que permita al consumidor o al comerciante almacenar información que se le transmita personalmente de forma que en el futuro pueda recuperarla fácilmente durante un período de tiempo acorde con los fines de dicha información y que permita la reproducción de la información almacenada sin cambios». Y el artículo 59 bis de la Ley: «todo instrumento que permita al consumidor y usuario y al empresario almacenar información que se le haya dirigido personalmente de forma que en el futuro pueda consultarla durante un período de tiempo acorde con los fines de dicha información y que permita su fiel reproducción. Entre otros, tiene la consideración de soporte duradero, el papel, las memorias USB, los CD-ROM, los DVD, las tarjetas de memoria o los discos duros de ordenador, los correos electrónicos, así como los mensajes SMS».

en ese soporte específico, antes de la celebración de dicho contrato, como mínimo la información precontractual sobre:

- las características principales de los bienes o servicios,
- la identidad del comerciante,
- el precio total,
- el derecho de desistimiento,
- la duración del contrato y,
- en el caso de contratos de duración indefinida, las condiciones de resolución.

Este apartado supone, a mi entender, un gran avance en el proceso informativo desde el momento en el que empezamos a hablar de información 'mínima' para poder adaptar las exigencias legales a las realidades tecnológicas de los dispositivos con tamaños reducidos. Sin perjuicio de que quede recorrido por andar, dado que la cantidad de información que deber proporcionarse sigue siendo mucha para el espacio informativo disponible.

Para completar esta información, la Directiva prevé que el comerciante deberá facilitar al consumidor las demás informaciones que figuran en el artículo 6, apartado 1, de forma previa a la celebración del contrato y de manera clara y comprensible. A esta información, que acabamos de describir, se le debe añadir, para los contratos electrónicos, los aspectos que recoge la Directiva de comercio electrónico.

Por otro lado, las actuales diferencias en los plazos de desistimiento en función de los Estados miembros y en lo que respecta a los contratos a distancia y los contratos celebrados fuera del establecimiento generan inseguridad jurídica y costes de cumplimiento para las empresas que realizan ventas transfronterizas. Por ese motivo, la Directiva unifica el plazo de desistimiento a todos los contratos a distancia y a los contratos celebrados fuera del establecimiento. Además, se introduce un formulario normalizado de desistimiento armonizado para el consumidor que simplifica el proceso de desistimiento y aporta una mayor seguridad jurídica: modelo que no podrá ser modificado por los Estados miembros y que para facilitar el acceso a los consumidores se deberá contemplar la posibilidad de ofrecer al consumidor la opción de cumplimentar el citado documento en línea en la web del comerciante y éste acusará recibo por correo electrónico sin demora del envío[21].

Como hemos visto, el derecho de desistimiento, es un elemento de la información debida en los contratos a distancia o en los contratos celebrados fuera del establecimiento, y en este sentido, Guillén Catalán[22] plantea la siguiente cuestión: ¿qué ocurre si no se

21 En este sentido la Ley 3/2014 armoniza a 14 días el plazo para ejercitar el derecho de desistimiento a través de la reforma del artículo 102 del TRLGDCU.

22 Ob. cit. Ver CAMARA LAPUENTE, S., (Director), (2011). Comentarios a las Normas de Protección de los Consumidores. Madrid: Colex. p. 615-695. Y COSTAS RODAL, L., (2013)

informa al consumidor de este derecho de desistimiento, ya que es un elemento añadido y particular a los datos relativos a la información general[23]?

Y responde:

> …en este caso el legislador comunitario sí ha establecido una única solución para todos los Estados miembros. Concretamente, el mencionado precepto establece, como consecuencia a la omisión del derecho de desistimiento, la ampliación del ejercicio de catorce días del citado derecho a doce meses después de la fecha de expiración del período de desistimiento inicial.

Visto así cuál es el panorama normativo comunitario vigente más próximo, el siguiente paso es analizar cómo nuestro legislador ha estado trabajando hasta la transposición de esta Directiva por la reciente Ley 3/2014, y en concreto, voy a estudiar cómo afecta esta nueva normativa al derecho de información.

3. EL DEBER DE INFORMACIÓN EN LA NORMATIVA ESPAÑOLA

El Apartado II de la Exposición de Motivos de la Ley que reforma el texto de consumidores, dispone que:

> La nueva ley supone un reforzamiento de la información al consumidor y usuario, a través de la ampliación de los requisitos de información precontractual exigibles en los contratos con consumidores y usuarios, que en el caso de los contratos a distancia y los contratos celebrados fuera del establecimiento del empresario han sido objeto de plena armonización por parte de la directiva.

Y más adelante, dice así:

> La ley regula también los requisitos formales de los contratos a distancia y de los celebrados fuera del establecimiento, y contempla como novedad la exigencia de que los sitios web de comercio indiquen de modo claro y legible, a más tardar al inicio del procedimiento de compra, si se aplica alguna restricción de suministro y cuáles son las modalidades de pago que se aceptan.
>
> Por otra parte, los requisitos de información exigibles con arreglo a esta ley vienen a completar los requisitos de información que se establecen en la Ley 17/2009, de 23 de noviembre, sobre el

---

El derecho de desistimiento en los contratos a distancia y en los contratos celebrados fuera de establecimiento mercantil en la proyectada reforma de la Ley de consumidores y usuarios. Revista Doctrinal Aranzadi Civil-Mercantil num.8/2013.

23 Además, en caso de que el empresario no facilite al consumidor la información sobre el derecho de desistimiento, se amplía el plazo para desistir del contrato hasta 12 meses después de la fecha de expiración del periodo inicial. La ley regula igualmente las obligaciones que asumen ambas partes del contrato en caso de desistimiento, así como los efectos del mismo respecto a los contratos complementarios.
Por otra parte, la ley contempla la posibilidad de que el empresario ofrezca al consumidor la opción de cumplimentar un formulario de desistimiento en línea, en cuyo caso deberá proporcionar sin demora indebida un acuse de recibo, por ejemplo, por correo electrónico.

libre acceso a las actividades de servicios y su ejercicio, y en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Hecha esta introducción puedo destacar que, como vamos a ver, la novedad más relevante, a mi entender, es que hasta la aprobación de esta Ley 3/2014, el texto de consumidores obligaba a los prestadores de servicios, como proveedores de contratación a distancia, a realizar una remisión normativa, dentro del mismo texto legal, concretamente del artículo 97, que regula el deber de información en la contratación a distancia, al artículo 60, que regula este mismo deber con carácter general para la contratación con consumidores, independientemente de que esta sea o no a distancia. Mientras el Anteproyecto de Ley mantenía la remisión normativa del artículo 97 al artículo 60, al igual que lo hacía el TRLGDCU, de forma que dividían la información debida al consumidor en la contratación a distancia entre los dos artículos y complicaban su conocimiento al prestador de servicios, ya el Proyecto de Ley de octubre de 2013 y ahora la Ley, eliminan esta remisión y considero que facilitan su cumplimiento por el prestador de servicios. Veamos las novedades introducidas:

Artículo 97 Información *precontractual* Antes de la reforma del 2014	Artículo 97. Información *contractual* de los contratos a distancia y los contratos celebrados fuera del establecimiento mercantil. Tras la reforma de 2014
1. Antes de iniciar el procedimiento de contratación y con la antelación necesaria, el empresario deberá suministrar al consumidor y usuario, de forma veraz y suficiente, la información prevista en el artículo 60 y además:	1. Antes de que el consumidor y usuario quede vinculado por cualquier contrato a distancia o celebrado fuera del establecimiento o cualquier oferta correspondiente, el empresario le facilitará de forma clara y comprensible la siguiente información:

Si analizamos los términos en cursiva, podemos destacar dos cuestiones importantes al respecto:

1ª Antes de la reforma el texto refundido hablaba de «antes de iniciar el procedimiento de contratación» expresión que no deja claro que estamos ya en la fase precontractual, y añade que «con antelación necesaria» término absolutamente inconcreto y que ha dado lugar a situaciones como la del Real Decreto 1906/1999[24], en el que se establecía un plazo de tres días previos para facilitar la información. Aspecto este

24 Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica y electrónica con condiciones generales. BOE núm. 313, de 31 de diciembre. Real Decreto derogado por la Ley 3/2014.

que ha sido muy criticado por la doctrina, por ejemplo, Paniza Fullana[25] comenta así esta exigencia:

> Tal vez con ello se esté desvirtuando la contratación electrónica: si quien visita una página web no puede concluir el contrato sino que tiene que esperar tres días, las características (rapidez...) de este tipo de contratos se pueden ver desvirtuadas con el establecimiento de este plazo mínimo. (...) Tener que esperar tres días para poder celebrar un contrato a través de medios caracterizados por su especial rapidez no parece la solución más idónea. (...) La consecuencia de su incumplimiento será el retraso en el inicio del cómputo del derecho de resolución hasta que las obligaciones referentes al deber de información estén totalmente cumplidas.

La nueva redacción fija un término, más acertado en nuestra opinión, cuando se refiere a que antes de que el consumidor «quede vinculado» lo cual describe un entorno más amplio y deja más claro el carácter previo de la información. Sin prejuicio de que esta información previa deba entenderse como parte integrante del contrato en el caso de que éste llegue a celebrarse.

2ª Mientras el Texto refundido se refería a información 'veraz y suficiente', después de la reforma lo hace como 'clara y comprensible', que a mi entender, como ya he referido, contribuyen mejor a la función informativa desde el momento en que persiguen garantizar la comprensión de la misma por el consumidor. ¿Cuándo si no una información puede ser suficiente si no es comprensible?

En relación con el contenido de la información, enumerado en el apartado 2 del artículo 97, si comparamos ambas redacciones encontramos que la Ley 3/2014 simplifica el deber de información en el sentido de que el empresario que realiza contratación a distancia debe acudir al artículo 97 para la información previa y al 98 para los requisitos formales y allí encuentra toda la información que debe proporcionar y los requisitos formales para incluirla. En este sentido, considero que la norma facilita el cumplimiento evitando remisiones normativas, entre su propio articulado, que en ocasiones complican o dificultan el cumplimiento. Y además, quiero destacar que los aspectos relacionados con la información que incluye el artículo 97 y que coinciden con los señalados en el artículo 60, quedan adaptados a la contratación a distancia, y por tanto a la contratación electrónica, de una forma más concreta para este tipo de contratación. Quiero señalar uno de los ejemplos más relevantes, a mí entender, es el referente a los datos relacionados con el empresario, veamos cómo quedan redactados tras la Ley 3/2014:

25 PANIZA FULLANA, A. (2003). Contratación a distancia y defensa de los consumidores. Granada: Comares. p. 185.

Art. 60 TRLGDCU	Artículo 97 TRLGDCU
b) La identidad del empresario, incluidos los datos correspondientes a la razón social, el nombre comercial, su dirección completa y su número de teléfono y, en su caso, del empresario por cuya cuenta actúe.	b) La identidad del empresario, incluido su nombre comercial. c) La dirección completa del establecimiento del empresario y el número de teléfono, número de fax y dirección de correo electrónico del mismo, cuando proceda, con objeto de que el consumidor y usuario pueda ponerse en contacto y comunicarse con él de forma rápida y eficaz, así como, cuando proceda, la dirección completa y la identidad del empresario por cuya cuenta actúa. d) Si es diferente de la dirección facilitada de conformidad con la letra c), la dirección completa de la sede del empresario y, cuando proceda, la del empresario por cuya cuenta actúa, a la que el consumidor y usuario puede dirigir sus reclamaciones.

Al hilo de lo que he comentado al tratar esta información en la Directiva 2011/83/UE, entiendo relevante para el entorno que estoy analizando, el entorno electrónico, que la letra c) del artículo 97 entre los datos de contacto del empresario, señale la necesidad de incluir la dirección de correo electrónico, cuando proceda con objeto de que el consumidor y usuario pueda ponerse en contacto y comunicarse con él de forma rápida y eficaz.

Por último, en cuanto al contenido, señalar que el artículo 97.5 se refiere a la integración de esta información como parte del contrato e incorpora el siguiente texto:

> Corresponderá al empresario probar el correcto cumplimiento de sus deberes informativos y, en su caso, el pacto expreso del contenido de la información facilitada antes de la celebración del contrato.

Este aspecto lo consideramos especialmente relevante dado que impone expresamente al empresario la carga de la prueba de haber cumplido el deber de información, lo que sin duda en la práctica nos llevará a configurar la forma de informar desde el diseño del proceso de contratación electrónica, trayendo a colación y por analogía un término usado en el ámbito de la privacidad, estaremos obligados a redoblar los esfuerzos en pro de la transparencia y de, si me permiten la expresión, la información 'desde el diseño'[26].

26 El Considerando 61 de la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011

Para terminar de analizar la información previa en la contratación electrónica, debemos acudir al artículo 27 de la LSSI[27] que, como ley sectorial, añade algunos matices en materia informativa cuando la contratación tiene lugar por medios electrónicos.

En segundo lugar encontramos el artículo 98 bajo la rúbrica de «requisitos formales de los contratos a distancia». La comparación entre la redacción anterior y posterior a la reforma de este precepto, me lleva a destacar cómo la nueva redacción hace referencias expresas a cuestiones relevantes en el entorno electrónico como son:

1. la exigencia de que el empresario deberá velar porque el consumidor y usuario, al efectuar el pedido, confirme expresamente que es consciente de que éste implica una obligación de pago. Así se desprende del Apartado 2 de este precepto que si la realización de un pedido se hace activando un botón o una función similar, el botón o la función similar deberán etiquetarse, de manera que sea fácilmente legible, únicamente con la expresión «pedido con obligación de pago» o una formulación análoga no ambigua que indique que la realización del pedido implica la obligación de pagar al empresario. En caso contrario, el consumidor y usuario no quedará obligado por el contrato o pedido.
2. También relacionada con la información sobre la obligación de pago, el Apartado 3, cuando destaca que los sitios web de comercio deberán indicar de modo claro y legible, a más tardar al inicio del procedimiento de compra, si se aplica alguna restricción de entrega y cuáles son las modalidades de pago aceptadas.
3. En cuanto a la celebración de los contratos a través de una técnica de comunicación a distancia en la que el espacio o el tiempo para facilitar la información son limitados, el Apartado 4 establece una serie de requisitos mínimos de información que deben ofrecerse al consumidor en todo caso. Este contenido mínimo hace referencia a las características principales de los bienes o servicios, la identidad del empresario, el precio total, el derecho de desistimiento, la duración del contrato y, en el caso de contratos de duración indefinida, las condiciones de resolución. Y a continuación insta al empresario a facilitar al consumidor y usuario las demás informaciones que figuran en el artículo 97 de una manera apropiada con arreglo al apartado 1.

El establecimiento de esta 'información mínima' supone un gran avance hacia la simplificación y la mejora del cumplimiento de la obligación de informar desde el mo-

– C7-0025/2012 – 2012/0011(COD)), dice así: «El principio de protección de datos desde el diseño requiere la integración de la protección de datos en todo el ciclo de vida de la tecnología, desde la primera fase de diseño hasta su despliegue final, su utilización y su eliminación definitiva».

27 No consideramos oportuno entrar a valorar aquí el contenido de este precepto dado lo limitado del espacio y dadas las novedades de la información en el TRLGDCU.

mento en el que el legislador se acerca al entorno que regula y establece una obligación que es más fácil de cumplir o al menos es 'más posible' de cumplir. Sin perjuicio de que todavía la carga informativa que se impone al empresario sea excesiva. Pero sin duda, debemos concluir el análisis de la evolución del deber de información en la contratación a distancia con consumidores con optimismo y con la opinión de que caminamos en la dirección correcta, aunque nos falte recorrido por andar.

Estas reglas formales de la información, en el caso de la contratación electrónica se completan con las reglas previstas en el artículo 28 de la LSSI[28].

Para concluir, diré que en mi opinión, debemos reconocer los avances de la reforma del texto de consumidores hacia una simplificación en las remisiones normativas y una definición del contenido de la información mínima. Y además, quiero señalar que en mi opinión parte de las soluciones futuras deben ir en la línea señalada sobre la información 'desde el diseño' y en las líneas que están siendo reclamadas desde ámbitos como el del uso de dispositivos de almacenamiento de datos[29], de una información por capas, que está siendo muy bien acogida por la industria, o el uso de iconos o imágenes informativas, como encontramos en el artículo 13 bis de la Resolución del Parlamento Europeo sobre el Reglamento de Protección de datos. En definitiva, el deber de informar no se queda en el contenido que debe incluir esa información, sino que va más allá y adquiere un papel muy relevante en el entorno electrónico, el cómo se facilite esa información y cómo pueda el consumidor tenerla a su disposición durante el tiempo que dure el contrato.

4. BIBLIOGRAFIA

Bednarz, Z., (2012) ¿Cómo influirá la nueva Directiva 2011/83/UE en el comercio electrónico?. En Actas del VIII Congreso Internacional Internet, Derecho y Política, celebrado los días 9 y 10 de julio de 2012, Universidad Oberta de Cataluña, (p. 167-180).

Bercovitz, A. y Bercovitz, R. (1987) Estudios jurídicos sobre protección de los consumidores. Madrid: Tecnos.

Camara Lapuente, S., (Director), (2011). Comentarios a las Normas de Protección de los Consumidores. Madrid: Colex.

Costas Rodal, L., (2013) El derecho de desistimiento en los contratos a distancia y en los contratos celebrados fuera de establecimiento mercantil en la proyectada

28 Sobre el que debo realizar la misma consideración que para el artículo 27.

29 Ver Guía sobre el uso de cookies, primera guía en Europa sobre la materia, publicada el 29 de abril de 2013 por la Agencia Española de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf.

reforma de la Ley de consumidores y usuarios. Revista Doctrinal Aranzadi Civil-Mercantil num.8/2013.

De Miguel Asensio, P., (2012) Obligaciones de información contractual en el comercio electrónico: noción de soporte duradero y significado de los enlaces. Fecha de consulta: 7 de julio 2012. En http://www.pedrodemiguelasensio.blogstop.com.

García Vicente, J.R., (2013). 10. La contratación con consumidores. En Bercovitz Rodríguez Cano, R., (Director), tratado de los contratos. Tomo II (2ª Ed., p. 1629-1790). Valencia: Tirant lo Blanch.

Gómez Segade, J.A. (1980). Notas sobre el derecho de información del consumidor. Revista Jurídica de Cataluña n. 3.

Guillén Catalán, R. (2012). La Directiva sobre los derechos de los consumidores: un paso hacia delante, pero incompleto. Diario La Ley (Nº 7801, de 20 Febrero de 2012).

Lasarte Álvarez, C. (2007) Manual sobre protección de consumidores y usuarios (3ª Ed.). Madrid: Dykinson.

Macías Castillo, A. (2005). Comentario al artículo 13 de la LGDCU. En Llamas Pombo, E. (Coordinador), Ley General para la Defensa de los Consumidores y Usuarios. Comentarios y Jurisprudencia de la Ley veinte años después (p. 501-538). Madrid: La Ley.

Paniza Fullana, A. (2003). Contratación a distancia y defensa de los consumidores. Granada: Comares.

BREACH OF INFORMATION DUTIES IN THE B2C E-COMMERCE –A COMPARATIVE ACCOUNT OF ENGLISH AND SPANISH LAW

Zofia Bednarz
PhD candidate, Law Faculty, University of Málaga, Spain

ABSTRACT: Electronic commerce plays nowadays a crucially important role in both professional and private activity of European consumers and businesses. The precontractual information duties are one of the factors that distinguish online contract formation between businesses and consumers from other ways of selling goods and services. The rules that apply to the e-commerce in the scope of the European internal market originate in two different legal systems, that is in the European law and in the national law. The aim of this study is to analyse and compare remedies available to consumers in the case of breach of information duties by the trader. The traditional contract law of Spain and England offers various remedies for not providing the other party with the due information. The interest in comparing those legal systems lies in the possible high number of cross-boarder transactions and the different nature of common and continental law. Even though the European legislation imposes numerous information duties, usually the remedies available for breach of those duties are left to the Member States' internal law, and therefore the analysis of the remedies available in the internal national law results necessary. The remedies that will be analysed and compared in this study are, under English law, misrepresentation, fraudulent, negligent or innocent, mistake, breach of statutory duty and breach of contract, and in what refers to Spanish law, remedies for vices of consent, for *culpa in contrahendo*, and for breach of contract.

KEYWORDS: Information duties, e-commerce, B2C distance contracts, breach of information duties, contract law remedies, misrepresentation, vices of consent, breach of contract.

1. GENERAL REMARKS ON THE INFORMATION DUTIES IN THE E-COMMERCE

Electronic commerce plays nowadays a crucially important role in both professional and private activity of European consumers and businesses[1]. Although the possibility of forming a contract online revolutionised the B2C commerce and the e-commerce is becoming one of the most popular ways of selling goods and services in the European

1 See Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *A coherent framework for building trust in the Digital Single Market for e-commerce and online services* COM(2011)942, p.1

internal market, it is still far from reaching its full potential, especially in what refers to cross-boarder transactions[2]. The obstacles that prevent the cross-boarder e-commerce from developing at desired level have been widely discussed by the academics, as well as by the European institutions[3]. Precontractual information duties, imposed by the directives which harmonise the Member States' contract law, may constitute one of those obstacles.

The precontractual information duties are one of the factors that distinguish online contract formation between businesses and consumers from other ways of selling goods and services[4]. However, the information duties were introduced in the contract law long before even the Internet started to be used by individuals as means of communication. The information asymmetry between consumers and traders has always been, together with the weaker economic power, an argument in favour of consumer protection[5]. The duties of information imposed on businesses are designed to correct these asymmetries, being in the meantime a tool that ensures the minimal possible restriction of the freedom of contract[6]. Moreover, the duties of information are especially important in the B2C e-commerce, as studies show that lack of trust, which could be remedied through providing relevant information, is one of the main factors responsible for discouraging consumers from online buying[7].

---

2 See Digital Agenda for Europe. Annual Progress Report 2011. 22 December 2011, p.3, where it is stated that 'Almost 9% of EU citizens ordered online in a different country [...]. However, as more than 40% of the EU population orders online in their own country, cross border e-commerce is not yet close to reaching its full potential' available online at http://www.ictventuregate.eu/wp-content/uploads/2012/01/dae_annual_report_2011.pdf

3 See for instance. Bednarz, Z. (2012). ¿Cómo influirá la nueva Directiva 2011/83/UE en el comercio electrónico? *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics.* Universitat Oberta de Catalunya, Barcelona, 9-10 July, 2012, p.155

4 Especially because e-commerce is one of so-called distance contracts, in this sense Marquez Lobillo, P. (2011). El consumidor en la contratación electrónica de servicios turístico. *Revista de Derecho Mercantil, núm. 282*, p. 212. Distance selling law applies therefore to the contracts formed online, see for instance Ruiz Muñoz, M. (2008). Tutela de los consumidores en el comercio electronico. *Revista de la Contratación Electronica, núm. 90*, p. 5

5 In this sense Hesselink, M. W. (2009). Towards a sharp distinction between B2B and B2C? On consumer, commercial and general contract law after the consumer rights directive. *Centre for the Study of European Contract Law Working Paper Series*, *No. 2009/06*, p. 33-34

6 See Lurger, B. (2005). The Future of European Contract Law between Freedom of Contract, Social Justice, and Market Rationality. *European Review of Contract Law, 4/2005*, p.442-468

7 See for example Ureña, A. (2011). *Estudio sobre Comercio Electrónico B2C 2011*, Observatorio Nacional de las Telecomunicaciones y de la SI, October 2011, p. 10 et seq.

The rules that apply to the e-commerce in the scope of the European internal market originate in two different legal systems, that is in the European law and in the national law. The specific duties of information were, and still are being introduced in the national legal systems by the European directives. Nevertheless, the national contract law also contains rules related to information duties. The e-commerce is by its nature perfect as means for cross-border transactions, hence the importance of the comparative approach in the analysis of the information duties in the B2C e-commerce. Scope and remedies available in the case of breach of those duties will be different in each national legal system[8], due to the important influence of the traditional contract law on the effectiveness of information duties. The legal systems being compared in this study, English and Spanish, represent two different European traditions: common law and civil law, distant in what refers to their origins and basic concepts, yet very close in practice due to cross-border online transactions being an everyday reality. Precontractual information duties and remedies available against breach of those duties constitute a field in which the difference between civil and common law is particularly evident[9].

The information duties mean that one contracting party is under a duty to inform, whilst the other party benefits from the right of information. The consumer can reasonably expect to be provided with accurate information in a comprehensible manner. Therefore the information duties in fact cover two concepts, a positive duty to provide information and a negative duty not to provide false, misleading or inaccurate information[10].

---

8 The Member States' legal systems represent different legal traditions, such as civil law, common law or Germanic law, which is especially important in the context of cross-border contracts. The duties of information are an important element of the European contract law, and the research in this field represents not only practical interest, but also theoretical: 'An investigation of the scope of the «duty to disclose» on a comparative law basis is most rewarding; it leads us straight to the heart of the philosophy underlying the law of contracts.' F. Kessler, E. Fine, 'Culpa in Contrahendo, Bargaining in Good Faith, and Freedom of Contract: A Comparative Study', *Harvard Law Review* 77, 1964, p.438

9 In this sense Wilhelmsson, T. (2003). Private Law Remedies against the Breach of Information Requirements of EC Law. In R. Schulze (ed.), *Informationspflichten und Vertragsschluss im Aquis Communautaire.* Tubingen 2003, p. 247

10 In this sense Sefton-Green, R. (2005). Duties to Inform versus Party Autonomy: Reversing the Paradigm (from Free Consent to Informed Consent)? - A comparative Account of French and English Law. In G. Howells, A. Janssen and R. Schulze (eds.), *Information Rights and Obligations,* Ashgate 2005, p. 174,
see also Zurilla Cariñana, M. A. (2009). El derecho de información del consumidor en los contratos con consumidores y usuarios en el nuevo TRLGDCU. *CESCO UCLM*, p.2, available at http://www.uclm.es/centro/cesco/pdf/comentarios/8.pdf,
in this sense also Miklaszewicz, P. (2008). *Obowiazki informacyjne w umowach z udzialem konsumentow,* Warszawa 2008, p. 32 et seq.

2. INFORMATION DUTIES IN THE EUROPEAN LAW

The *aquis communautaire* on the B2C e-commerce establishes various information duties. The most important directives in this context are Directive 2000/31/EC on electronic commerce and Directive 2011/83/EU on consumer rights, however some provisions of other directives may also be relevant[11]. The Directive on e-commerce in its articles 5, 6 and 10 lists the information requirements that should be met by the service provider, these requirements include information relating to the trader himself, to the service provided and to the formation of contract. This Directive is subject to minimum harmonisation, Member States can therefore adopt more stringent provisions than those established in the Directive.

The Directive on consumer rights, adopted in October 2011, was intended to revolutionise online shopping[12] and contains various requirements in what refers to information that should be provided before the formation of a distance contract, which concept includes also online contracts. Article 6 of the Directive contains a list of information requirements, which again can be grouped as those referring to the identity of the trader, characteristics of the good or service offered and the way in which the contract is made. Nevertheless, the list of information duties is much more developed in this Directive, as it contains also information requirements related to the right of withdrawal, as well as to the costs, such as delivery and returning costs. Those provisions are subject to the full harmonisation, prohibiting Member States from adopting both less and more stringent provisions than those stated in the Directive[13]. The full harmonisation approach to information requirements raises doubts as to relation between the very specific information duties listed in the Directive and more general concepts of Member States' law[14], such as misrepresentation or fraud, which are to be mentioned below.

---

11 See for example: Directive 2002/65/EC concerning the distance marketing of consumer financial services, Directives 84/450/EEC and 97/55/EC in what refers to advertising as precontractual information, Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and Directive 93/13/EEC on unfair terms in consumer contracts.

12 See for example the recital (5) of the Directive 2011/83/UE, other provisions of the Directive also clearly show its importance the e-commerce, see for example art.6.1 (s) on the digital content or art. 19 that prohibits additional fees for the use of specific means of payment, which has been a common practise in the online shopping.

13 However, according to the article 6.8 Member States are allowed to impose additional information requirements in accordance with the Directive 2000/31/EC, which, to some extent, compromises the full harmonisation approach.

14 In this sense Micklitz, H. W., Reich, N. (2009). Cronica de una muerte anunciada: The Commission Proposal for a «Directive on Consumer Rights». *Common Market Law Review,* 46: 471–519, p. 17

Even though the directives impose numerous information duties, they usually leave the remedies available for breach of those duties to the Member States' internal law[15]. For example, the Directive on consumer rights in its art. 24.1 requires Member States to take all measures necessary to ensure the implementation of its provisions, which includes also the information requirements[16]. This solution makes it essential to analyse the national internal law to be able to decide which remedies are available for consumers in the case of a breach of information duties. The character of those remedies, for example a question whether contract or tort law applies, is of crucial importance also for determining the law applicable in the case of eventual cross-boarder dispute[17].

However, the concept of the European law covers not only the *aquis communautaire*, but also the *soft law* instruments, such as PECL[18] or DCFR[19]. Those instruments form an important part of the European law, although their rules are more of a model and guidance, especially in what refers to consumer contracts, where law applicable is usually positive national or European law. Section 1 of Chapter 3, Book II of DCFR contains rules referring to information duties and the last article of this Section, II.-3:109 establishes remedies for their breach. These remedies include the extension of the withdrawal period[20] and remedies available in the case of non-performance of obliga-

15 Nevertheless, there are some exceptions, for instance in what refers to the information on the right of withdrawal, see Directive 2011/83/EU article 10, also the information on the costs is specifically protected by this Directive in the article 6.6

16 It has been widely criticized, see for instance Guillen Catalan, R. (2012). La Directiva sobre los derechos de los consumidores: un paso hacia delante, pero incompleto. *Diario La Ley, no 7801, Sección Tribuna*, 20 Feb. 2012, p.3 et seq. This has been observed as a general trend before, Wilhelmsson, T. (2003). Private Law Remedies...*op. cit.* p. 247, explains that '[…] remedies for breaches of information duties are often the responsibility of national law. Usually, the Directives only require Member States to ensure that adequate and effective means exist to ensure compliance.'

17 The conflict rules applicable would be the law of the consumer's residence, according to Brussels Regulation 44/2001 and Rome II Regulation 864/2007, as claims out of *culpa in contrahendo* form part of the tort law, for more details see for example Micklitz, H. W., Reich N. (2009). Cronica de una muerte anunciada...' *op.cit*, p.18

18 Principles of European Contract Law, a private compilation of uniform legal principles for reference, available at http://www.storme.be/PECL.html

19 Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference, available at http://ec.europa.eu/justice/contract/files/european-private-law_en.pdf, however apart from PECL and DCFR there are also other compilations that should be studied in detail, such as ACQP, Principles of the Existing EC Contract Law (Aquis Principles), and especially Contract I: Pre-Contractual Obligations.

20 According to the article II.-3:109(1) available to especially vulnerable consumers if a contract was subject to the right of withdrawal

tions, such as damages, performance withholding or right to enforce performance[21]. It can be therefore assumed that information duties are perceived as actionable obligations in the DCFR, although their nature may vary between contractual and tortious.

3. REMARKS ON THE NATIONAL LAW AND REMEDIES IT OFFERS

The information duties existing in the national law are of double origin and nature. On the one hand the European law, harmonising Member States' legal systems, has imposed detailed, specific information requirements that can be found usually in the national legislation that implements directives into the internal law. On the other hand, the traditional national contract law usually contains by itself various rules linked to the precontractual duty to disclose. These two types of duties coexist in internal law, which may cause various problems. First of all, an important issue, already mentioned above, is the full harmonisation approach used in the 2011/83/EU Directive. The problems may arise when the general duty of fair dealing and good faith present in the national internal legal system implies a wider than the Directive scope of the duty to inform. Such a situation may be even considered a violation of the full harmonisation principle[22]. Secondly, the nature of the information duties, that is whether they are obligations of a contractual or different character, also poses a problem, as internal systems may catalogue them differently. It would then influence for instance jurisdictional rules applicable[23], as well as lead to other important consequences[24].

Since Member States are obliged to implement the European directives together with the information requirements they establish into the national law, the national acts implementing those directives have to contain information duties. In what refers to the e-commerce the most relevant for purposes of this study would be those Acts of

21 See Book III, Chapter 3 of the DCFR

22 Mak, V. (2012). Full Harmonization in European Private Law: A Two-Track Concep. *European Private Law Review, 20*(1), 2012, p. 213 et seq, points out that the European Court of Justice, in the context of the 93/13/CEE Directive, decided to apply the '*result – oriented'* approach to the full harmonisation in the cases VTB-VAB NV / Total Belgium NV (C-261/07), Plus Warenhandelsgesellschaft (C-304/08) and Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG (C-540/08). This approach to full harmonisation means that Member States are not allowed to apply the internal law, even if it is general contract law, to the matters covered by the directive.

23 See for instance European Court of Justice C-26/91, Jakob Handte & Co. GmbH v Traitements Mécano-chimiques des Surfaces SA., Judgment of the Court of 17 June 1992.

24 For example, under English law damages are measured differently for contractual and tortious liability. Under Spanish law, the time to present an action for damages in tort is 1 year, whilst for breach of contract it is up to 15 years.

Parliament which implement the Directive on distance contracts and the Directive on e-commerce.

The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013[25] in the schedule and regulation 13 establish information duties. Those requirements form groups that contain certain types of information, for instance information about the trader, about the goods or services, about the sale itself, and about the right of withdrawal. The correspondent Spanish Act of Parliament, TRLGDCU[26], imposes similar duties in its articles 60, 97 and following. In what refers to the online B2C transactions, the legislation that should be analysed is The English Electronic Commerce Regulations 2002[27] and on the Spanish side the LSSI[28]. All those Acts establish a broad scope of information duties. The question that rises is how those duties are enforced by the national law and which remedies are available to consumer for their breach.

The traditional approach to liability in private law is dichotomal, it is either arising from contract or from tort and it always aims at repairing the damage caused to the other party[29]. However, in the B2C contractual relationships, the breach of information duties will not always cause economically evaluable damage to consumers, and this situation should not result in depriving them of any remedies. Moreover, the important issue is the economic efficiency of the remedies available for a consumer, since importance of a particular contract for the consumer and for the trader is different. The former is pursuing a good or a service which is unique and necessary for his personal purposes, while for the latter the particular contract is just one of many formed that day. Therefore the remedies appropriate for consumers in the case of a breach of information duties often will not fit the traditional private law liability.

Information duties implemented in the national internal law become its part and therefore are subject to general rules of the traditional contract law. Civil law systems, as in Spanish case, tend to recognize a general duty to inform the other contracting party. The consumer's right to be informed and correspondent information duties in Spanish

25 The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013, Statutory Instrument 2013 No. 3134 implementing the Consumer Rights Directive 2011/83/EU.

26 Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, as amended by the Ley 3/2014, de 27 de marzo.

27 The Electronic Commerce Regulations 2002 (Statutory Instrument 2002/2013).

28 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

29 See for instance Kuhne, G. (1990). Reliance, Promissory Estoppel and Culpa In Contrahendo: A comparative Analysis. *Tel Aviv University Studies in Law*, 10, Tel Aviv 1990, p. 279.

legal system reach beyond the contract law as they are established in the supreme set of norms, the Spanish Constitution[30]. The contract law itself is based on the principle of good faith, resulting from articles 7.1 and 1258 of the Spanish Civil code, and this principle is interpreted in this way that it gives rise to a duty to disclose material information before the conclusion of a contract[31]. In this context the information duties established in the Acts of Parliament implementing European directives can be seen as a specific application of general principles.

In what refers to English law, however, the analysis of the information duties is more complicated, as English law recognises no general duty to disclose. The authority for this rule in English law is the classic case Smith v Hughes [1871][32] where Blackburn J explained that 'there is no legal obligation on the vendor to inform the purchaser that he is under mistake, not induced by the act of vendor'[33]. Despite the attempts to introduce a general duty to inform in the English law, such a doctrine, apart from specific application to *uberrimae fidei* contracts, was never accepted[34]. This position was confirmed in a more recent case National Westminster Bank v Utrecht – America Finance Co. [2001], where it was stated again that 'in England a contract like TOA is not a contract *uberrimae fidei* and neither party owes a duty to disclose material facts to the other.'[35].

Nevertheless, if there is a duty to inform, like in the B2C e-commerce, where specific information requirements apply, then not providing any information or providing information that is untrue, not accurate or defective in any way, will constitute a breach

30 See for instance Lasarte Alvarez, C. (2008). La protección del consumidor como Principio General de Derecho. In A. Monserrat Quitana (ed.), *Nuevos derechos fundamentales en el ámbito del Derecho privado,* Consejo General del Poder Judicial 2008, p. 71 where the author refers to the article 51 of the Spanish Constitution.

31 In this sense for example Picatoste Bobillo, J. (2011). El derecho de información en la contratación con consumidores. *Actualidad Civil no 4,* febrero 2011, p. 393 who considers that the precontractual duty to inform was implicitly included in the Civil code as an obligation to act accordingly to the principle of good faith. Other authors confirm this point of view, consult for example: Guillén Catalán, R. (2010). *El regimén jurídico de la oferta contractual dirigida a los consumidores (Adaptada al Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el TRLGDCU*, Colegio de Registradores de la Propiedad y Mercantiles de España, Centro de Estudios, 2010, p. 28 et seq., also in this sense Zurilla Cariñana, M. A. (2009). El derecho de información del consumidor...*op.cit.,* p.1 et seq.

32 Smith v Hughes [1871] LR 6 QB 597.

33 At 597.

34 As to attempts see for instance Lloyds Bank Ltd v Bundy [1974] EWCA Civ 8, per Denning LJ.

35 National Westminster Bank v Utrecht America Finance Co. [2001] 3 All ER 733, 750, para 51, per Clarke LJ.

of that duty, also under English law[36]. Moreover, even when there is no obligation on the party to inform, giving false information is not allowed by the courts[37]. The remedies available in common law and in civil law are quite different, when analysed from a strictly legal, technical point of view, but their purpose and final outcomes are often similar. Two situations have to be distinguished, first, where no information was given to a consumer despite the legally imposed duty to disclose, and second, where information provided to a consumer was misleading. The most important remedies for breach of information duties under English and Spanish law are presented below.

3.1. Lack of information that should have been provided

In the case of non-disclosure, i.e. when a piece of information that should have been provided was omitted, various remedies are available to a consumer. Failure to provide some specific information often leads to applicability of particular remedies, which is a direct consequence of implementation of the European law. Those situations will be therefore similar in both Spanish and English law. For instance, failure to provide information on the consumer's right to withdraw from the distance contract will result in the withdrawal (cancellation) period extension to up to 12 months, according to the regulation 31 Consumer Contracts Regulations 2013 and article 105 of the TRLGDCU as amended on March 27, 2014; both these pieces of legislation implement the Consumer Rights Directive 2011/83/EU, and in this particular case its article 10.

Nevertheless, European directives often fail to establish specific remedies for the breach of the duty to inform[38]. In such case it is Member States' responsibility to ensure the effectiveness of the European rules and therefore new remedies have to be introduced for each type of information duty, or, more commonly, the national general private law and traditional remedies it offers will become applicable.

As mentioned above, English law in principle does not recognise a general duty to disclose, and therefore non-disclosure does not imply a breach of any duty towards the other contracting party. Nevertheless, in the case of consumer contracts, the informa-

36 In this sense for instance Sefton-Green, R. (2005). Duties to Inform versus Party Autonomy... *op.cit.*, p. 174.

37 An illustration is given by Sefton-Green, R. (2005). Duties to Inform versus Party Autonomy... *op.cit.*, p. 174 footnote 18, a clause excluding liability for non-disclosure was held valid in the National Westminster Bank v Utrecht America case, while excluding liability for misrepresentation would have to satisfy the reasonableness provisions of Section 3 Misrepresentation Act 1967.

38 In this sense for example Wilhelmsson, T. (2003). Private Law Remedies...*op. cit.*, p. 247, '*However, remedies for breaches of information duties are often the responsability of national law. Usually, the Directives only require Member States to ensure that adequate and effective means exist to ensure compliance.'*

tion duties are usually imposed by statutes. In some very limited cases, where the statute establishes so itself, the breach of statutory duty can lead to the damages being awarded to the aggrieved party[39], however this does not necessarily mean that the contract could be rescinded. The remedy offered in similar situations by the Spanish law is equally limited, however for different reasons. The applicable Act of Parliament, TRLGDCU[40], does not establish any specific remedy in the case of a breach of duty to inform. This can be considered to be an incoherent legislative solution[41], as the Spanish Act of Parliament LOCM[42], replaced by the TRLGDCU in what refers to consumer contracts, in its articles 44.5 and 47 offers a claim for rescission of contract to the aggrieved party in the case of breach of some important information duties in the distance contracts.

Where no remedy for breach of statutory duty applies, the aggrieved party may turn to the general contract and tort law institutions. For instance, in some cases the information that should have been provided before the conclusion of the contract forms part of the contract itself and the duty to provide it becomes one of the terms of the contract. Breach of this kind of information duties will then amount to the breach of contract. In what refers to the English law, such situation may occur if the duty to provide information is considered to be a term of the contract. Especially terms implied in law should be taken into account as their breach will amount to the breach of contract, as in the case of any other term of contract. Acts of Parliament concerning consumer contracts often imply terms related to the information duties, as to duties that arise out of certain types of contracts.

In what refers to Spanish law, there are authors who opt for the remedies for breach of contract in the case of breach of information duties. Although the information duties are considered to be precontractual duties, their breach will amount to the breach of contract. This is for example the reasoning of P. Valés Duque, who explains that 'In what refers to the information duties, it has to be considered that, to the liability rising from the breach of those precontractual duties […], the law of contract should apply'[43].

---

39 See for example reg. 13, The Electronic Commerce Regulations 2002 (Statutory Instrument 2002/2013), according to which an action for tort of breach of statutory duty can be brought when the precontractual information was not provided.

40 See footnote 26.

41 See for instance Picatoste Bobillo, J. (2011). El derecho de información en la contratación con consumidores...*op.cit.,* who consideres this to be a legal loop: 'estamos ante un olvido del legislador en la tarea de refundición del TRLDCU por lo que será aplicable la regulación de la facultad resolutoria por incumplimiento de los deberes de información del art. 44 LOCM (Ley de Ordenación del Comercio Minorista)'.

42 Ley 7/1996, de Ordenación del Comercio Minorista.

43 Author's translation from: Valés Duque, P. (2012). *La responsabilidad precontractual,* Madrid 2012, p. 118: '*En cuanto a los deberes de información, ha de admitirse que la responsabilidad derivada del incumplimiento de estos deberes precontractuales...ha de regirse por las normas contractuales...*'

The action for misrepresentation should also be taken into account in the case of breach of information duties under the English law. Nevertheless, it will be applicable above all to the cases where misleading information has been provided, as analysed in the next section of this study, hence the scope of this action is limited to when a representation was made, that is when some information, although false, has been provided. However, an implied representation may be taken into account by the courts given the known characteristics of the actual representee, especially if he is a consumer[44]. Moreover, in some cases a representation may be inferred from conduct, circumstances or custom, and therefore non-disclosure could amount to misrepresentation[45].

Not providing information to the other party before the conclusion of a contract may also induce a mistake of that party in what refers to essential terms of contract. However, only one contracting party would be labouring under a mistake and therefore the doctrine of common mistake would not apply. Instead, the doctrine of unilateral mistake would result applicable. The contract on objectively[46] determined terms will be enforced by the courts. Such mistake would be actionable only if one party was genuinely mistaken as to the terms of the contract[47], therefore the duty to provide information would have to be considered as a contractual term to give rise to this action. In what refers to Spanish law, traditionally the doctrine of vices of consent, *vicios del consentimiento*, is taken into account. Especially the action *dolo,* fraud, may be brought in the case of non-disclosure, that is when the information was not provided.

As far as the Spanish legal system is concerned, the institution of *culpa in contrahendo*[48], precontractual liability for breaching the precontractual good faith, should be taken into account as well. The *culpa in contrahendo* principle offers remedies in the case of a harmful conduct that occurs during a formation period of a contract[49] and gives rise to tortiuos liability under art. 1902 of Spanish Civil Code. Hence, the remedy available would be damages for the loss suffered by the aggrieved party. Nonetheless, *culpa in con-*

44 See Raiffeisen Zentralbank Osterreich AG v Royal Bank of Scotland Plc [2010] EWHC 1392 at 81.

45 See for instance Peel, E. (2011). *Treitel The Law of Contract*, 13th edition 2011, p. 366.

46 See Smith v Hughes [1871] LR 6 QB 597 the leading case on the meaning of objectivity.

47 See Poole, J. (2012). *Textbook on contract law,* Oxford University Press 2012, p. 99.

48 In this sense explains Gómez Calle, E. (1994). that '[…] hay que contar con el régimen general de la responsabilidad precontractual o por *culpa in contrahendo* de quien infringe sus deberes de información. Su fundamento positivo ha de situarse en nuestro ordenamiento en el art. 1902 CC' in *Los deberes precontractuales de información,* Madrid 1994, p. 134.

49 See Hage-Chahine, N. (2012). Culpa in Contrahendo in European Private International Law: Another Look at Article 12 of the Rome II Regulation. *Northwestern Journal of International Law & Business, 32*(3), p. 452.

trahendo covers wide group of different precontractual conducts[50] and the only relevant for the purposes of this study is when the contract formed between business and consumer is disadvantageous to the latter due to the breach of information duties by the trader. In such case the consumer would be entitled to either judicial reconstruction of the contract on more beneficial terms, or to the rescission and damages, when applicable[51].

3.2. Consumer induced into the contract by misleading information

When a party was given false or misleading information in the precontractual period, the traditional remedies, already mentioned above, are action for misrepresentation and, in some limited cases, mistake, under English law and vices of consent under Spanish law. An actionable misrepresentation is a false statement of fact or law which induced the representee, a consumer in this case, to enter into a contract[52]. The remedies available in the case of mirepresentation vary depending on the grounds for misrepresentations, which can be fraudulent, negligent or innocent. In what refers to vices of consent, *el dolo*[53], which is a mistake induced by the other party, would be the most relevant in the analysed context.

If the information provided by the other party was fraudulently misleading, English law offers a possibility of bringing a claim for fraud, providing that certain conditions are met. It must be shown that the representor knew a statement was untrue, had no belief in its truth, or was reckless as to whether it was true or false[54]. The remedies available for fraud are damages under the tort of deceit and rescission of contract[55]. Both remedies can be pursued providing it doesn't result in recovering twice for the same loss[56]. In similar circumstances under Spanish law an action for *dolo* can be taken, since the art. 1269 of the Spanish Civil Code defines '*dolo*' as 'fraudulent misrepresentation [which] exists where, with insidious words or machinations on the part of one of the contracting parties, the other is induced to enter into a contract which he would not have done without them'[57]. The Civil Code distinguishes between the *dolo grave* (serious

50 See García Rubio, M. P., Otero Crespo, M. (2010). La responsabilidad precontractual en el Derecho contractual europeo. *InDret* 2/2010, p. 33 et seq.

51 See García Rubio, M. P., Otero Crespo, M. (2010). La responsabilidad precontractual...*op.cit.*, p. 53.

52 See for example Peel, E. (2011). *Treitel The Law of Contract...op.cit.*, p.361.

53 See art. 1269 of Spanish Civil Code.

54 Derry v Peek [1889] 5 T.L.R. 625.

55 Doyle v Olby [1969] 2QB 158, Smith New Court Securities v Scrimgeour Vickers [1996] 3 WLR 1051.

56 Archer v Brown [1984] 2 All ER 267.

57 English translation of the Spanish Civil Code by Sofía de Ramón-Laca Clausen, Ministerio de Justicia (Spanish Ministry of Justice).

fraud), which occurs when the representee wouldn't have entered the contract if it hadn't been for the misrepresentation of the other party, and *dolo incidental*, when the representee would have entered the contract anyway, but on better conditions. Both types of *dolo* entitle the damaged party to recover its loss, but only *dolo grave* renders the contract void and allows to claim its rescission[58].

The main difference between fraudulent misrepresentation and *dolo* is the scope of those actions. Under English law only statements, with some exceptions regarding for example conducts, can amount to representations[59], while *dolo* can also be constituted by silence, that is by simple non-disclosure[60]. Another interesting difference between the effects of fraudulent misrepresentation and *dolo* is that the former makes the contract voidable, and the latter void. The voidable contract exists from the beginning and the effects of the rescinded contract are recognised to have taken place, whilst the void contract never existed and therefore can not produce any effects[61].

English law offers remedies for the representee also when the misrepresentation was made negligently or even innocently by the representor. Negligent misrepresentation covers situations where representations were made without due care but not fraudulently by the representor. The remedies available are damages and rescission, with two possible claims for damages available for representee, a claim in tort for negligent misstatement[62] and a claim for damages under s.2(1) Misrepresentation Act 1967. The difficulty with the claim for damages for negligent misstatement at common law is that the misrepresentee has the burden of proving both the existence of the duty of care and its breach. Under Misrepresentation Act the burden of proof is reversed and the defendant has to show that he had reasonable grounds to believe that the statement he made was true. In the case of innocent misrepresentation, the aggrieved party is entitled to rescission of the contract and to an indemnity intended to restore the parties to the position before entering the contract[63].

58 Lacruz Berdejo, J. L. et al. (2007). *Derecho de obligaciones. Volumen Primero: Parte general. Teoría del contrato,* Madrid 2007, p. 368.

59 See for instance Peel, E. (2011). *Treitel The Law of Contract..op.cit.,* p. 366.

60 In this sense Guillen Catalán, R. (2012). La Directiva sobre los derechos de los *consumidores... op.cit.,* p.4.

61 With some exceptions regarding third party's rights.

62 The common law tort of negligence was extended in 1964 by the House of Lords to the field of negligent statements which cause loss, see Hedley Byrne & Co. Ltd v Heller & Partners Ltd [1964] AC 465.

63 See for instance Poole, J. (2012). *Textbook on contract law...op.cit*, p. 521.

Under Spanish law false information provided negligently by the representor gives rise to liability under the previously mentioned doctrine of *culpa in contrahendo,* as action for *dolo* may be brought only if the false representation was made intentionally.

Nevertheless, in what refers to consumer contracts, an action for misrepresentation has a great disadvantage. The representee has to demonstrate that the false statement induced them to enter the contract[64], which may constitute an important obstacle in practice. The same refers to actions offered by Spanish law, the burden of proof rests on the aggrieved party.

The false, incomplete or misleading information provided before the conclusion of the contract may as well become a term of the contract, and therefore the breach of this kind of information duties will amount to the breach of contract, similarly to the case of non-disclosure discussed above.

Under English law it is important to determine if the breach of information duties gives rise to the claim for misrepresentation or for the breach of contract, as the assessment of damages will be different[65]. In what refers to liability for misrepresentation in tort, the damages awarded should put the claimant into the position he would have been in, had not the tort been committed, that is as if the representation had not been made. On the other hand, the damages for the breach of contract put the claimant into the position in which he would have been, had the contract been correctly performed, as if the statement had been true. Moreover, the rescission of contract is always granted in the case of actionable misrepresentation, while the breach contract does not always give right to set the contract aside[66]. Therefore it is essential to distinguish statements that are representations from those that can be regarded as terms of contract. The main distinction between terms and representations lies in the intention with which the statement was made. Although the approach adopted by courts in what refers to intention is objective, it is often difficult to determine the nature of the statement, as there are numerous principles, none of which decisive, to guide the court in deciding on this matter[67].

4. CLOSING REMARKS

The information duties at the same time constitute an obstacle to the development of the cross-boarder e-commerce and a factor that could contribute to the increase of

64 Horsfall v Thomas [1862] 1 H&C 90.

65 See for instance Peel, E. (2011). *Treitel The Law of Contract...op.cit.,* p. 390.

66 See for instance McKendrick, E. (2011). *Contract law,* Palgrave Macmillan Law Masters 2011, p. 151.

67 See McKendrick, E. (2011). *Contract law...op.cit.,* p. 149 and the case mentioned there, Heilbut, Symons & Co v Buckleton [1913] AC 30, 50 – 51 by Moulton L.

trust of both consumers and traders. Electronic B2C transactions differ from the traditional commerce as the bargaining power of the contracting parties is even less equal than normally, and therefore the European legislator seeks to boost the e-commerce by addressing the issue of the information duties. Nevertheless, those duties without effective remedies available for their breach in the national legal systems would not be observed by the traders.

It has to be taken into account, however, that those duties do not present any particular novelty in European legal systems, and the traditional contract law in both Spain and England offers various remedies for not providing the other party with the due information. The interest in comparing those legal systems lies in the possible high number of cross-boarder transactions and the different nature of common and continental law, which may be confusing for the consumers seeking remedies in the case of breach of their rights.

The main difference between the compared systems is that the English law does not recognise a doctrine of good faith and fair dealing and therefore neither a general duty of disclosure, while the Spanish contract law is based on those principles. However, the effectiveness of the remedies offered by both systems is similar, it can be therefore concluded that the differences are more of technique than result[68].

5. BIBLIOGRAPHY

Bednarz, Z. (2012). ¿Cómo influirá la nueva Directiva 2011/83/UE en el comercio electrónico? *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics.* Universitat Oberta de Catalunya, Barcelona, 9-10 July, 2012

García Rubio, M. P., Otero Crespo, M. (2010). La responsabilidad precontractual en el Derecho contractual europeo. *InDret* 2/2010

Gómez Calle, E. (1994). *Los deberes precontractuales de información,* Madrid 1994

Guillén Catalán, R. (2010). *El regimén jurídico de la oferta contractual dirigida a los consumidores (Adaptada al Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el TRLGDCU,* Colegio de Registradores de la Propiedad y Mercantiles de España, Centro de Estudios, 2010

Guillen Catalan, R. (2012). La Directiva sobre los derechos de los consumidores: un paso hacia delante, pero incompleto. *Diario La Ley, no 7801, Sección Tribuna*, 20 Feb. 2012

68 See McKendrick, E. (2011). *Contract law...op.cit.,* p. 219 et seq.

Hage-Chahine, N. (2012). Culpa in Contrahendo in European Private International Law: Another Look at Article 12 of the Rome II Regulation. *Northwestern Journal of International Law & Business, 32*(3)

Hesselink, M. W. (2009). Towards a sharp distinction between B2B and B2C? On consumer, commercial and general contract law after the consumer rights directive. *Centre for the Study of European Contract Law Working Paper Series, No. 2009/06*

Kuhne, G. (1990). *Reliance, Promissory Estoppel and Culpa In Contrahendo: A comparative Analysis. Tel Aviv University Studies in Law, 10, Tel Aviv 1990*

Lacruz Berdejo, J. L. et al. (2007). *Derecho de obligaciones. Volumen Primero: Parte general. Teoría del contrato,* Madrid 2007

Lasarte Alvarez, C. (2008). La protección del consumidor como Principio General de Derecho. In A. Monserrat Quitana (ed.), *Nuevos derechos fundamentales en el ámbito del Derecho privado,* Consejo General del Poder Judicial 2008

Lurger, B. (2005). The Future of European Contract Law between Freedom of Contract, Social Justice, and Market Rationality. *European Review of Contract Law, 4/2005*

Mak, V. (2012). Full Harmonization in European Private Law: A Two-Track Concep. *European Private Law Review, 20*(1), 2012

Marquez Lobillo, P. (2011). El consumidor en la contratación electrónica de servicios turístico. *Revista de Derecho Mercantil, núm. 282*

McKendrick, E. (2011). *Contract law, Palgrave Macmillan Law Masters 2011*

Micklitz, H. W., Reich, N. (2009). *Cronica de una muerte anunciada: The Commission Proposal for a «Directive on Consumer Rights». Common Market Law Review, 46: 471–519*

Miklaszewicz, P. (2008). *Obowiazki informacyjne w umowach z udzialem konsumentow, Warszawa 2008*

Peel, E. (2011). *Treitel The Law of Contract*

Poole, J. (2012). *Textbook on contract law, Oxford University Press 2012*

Picatoste Bobillo, J. (2011). *El derecho de información en la contratación con consumidores. Actualidad Civil no 4, febrero 2011*

Ruiz Muñoz, M. (2008). Tutela de los consumidores en el comercio electronico. *Revista de la Contratación Electronica, núm. 90*

Sefton-Green, R. (2005). Duties to Inform versus Party Autonomy: Reversing the Paradigm (from Free Consent to Informed Consent)? - A comparative Account of French and English Law. In G. Howells, A. Janssen and R. Schulze (eds.), *Information Rights and Obligations,* Ashgate 2005

Ureña, A. (2011). Estudio sobre Comercio Electrónico B2C 2011, *Observatorio Nacional de las Telecomunicaciones y de la SI,* October 2011

Valés Duque, P. (2012). *La responsabilidad precontractual,* Madrid 2012

Wilhelmsson, T. (2003). Private Law Remedies against the Breach of Information Requirements of EC Law. In Reiner Schulze (ed.), *Informationspflichten und Vertragsschluss im Aquis Communautaire.* Tubingen 2003

Zurilla Cariñana, M. A. (2009). El derecho de información del consumidor en los contratos con consumidores y usuarios en el nuevo TRLGDCU. *CESCO UCLM*

PROTECCIÓN DE LOS CONSUMIDORES ORIENTADA A PROCESOS MÁQUINA A MÁQUINA

Jose Manuel Pérez Marzabal
Abogado. MTNProjects.com
Consultor UOC

RESUMEN: Esta comunicación investiga algunos problemas jurídicos específicos de la protección de los consumidores en el contexto del denominado «Internet de las Cosas». El autor sostiene que mientras que la protección del consumidor y la regulación aplicable pueden responder a algunas de las dificultades jurídicas que se plantean en la actualidad, las evoluciones del comercio electrónico tradicional en un contexto de omnipresencia computacional y del Internet de las Cosas, a su vez plantean nuevos retos legales al régimen de los contratos de adhesión y la protección de los consumidores.

PALABRAS CLAVE: Internet de las Cosas, protección de los consumidores, contratación electrónica.

1. INTRODUCCIÓN

El desarrollo del comercio electrónico desempeña un papel fundamental en el propio desarrollo de la sociedad red[1]. Si las empresas y los ciudadanos se habitúan a realizar transacciones a través de la Red, las ventajas en ahorro de costes y mejora de la competitividad se traducirán en crecimiento económico. En este contexto, el advenimiento del Internet de las Cosas («IoT») tendrá repercusiones importantes sobre el desarrollo de Internet[2].

Las proyecciones apuntan a que en 2017, una familia con dos hijos adolescentes podría tener 25 objetos conectados a Internet. Las empresas modificarán radicalmente el proceso de diseño y producción de máquinas y dispositivos, iniciándose a partir del tipo de datos que necesitan para operar de manera eficiente y eficaz y, posteriormente, basar la producción de la máquina o dispositivo sobre dicho parámetro. La predicción

1 Castells, M. (2010), *The rise of the Network Society*, 2ª Edición, Oxford, Wiley-Blackwell.

2 OECD (2012), *Machine-to-Machine Communications: Connecting Billions of Devices*, OECD Digital Economy Papers, N. 192, OECD Publishing, recuperado el 1 de marzo de 2014, en http://www.oecd-ilibrary.org/docserver/download/5k9gsh2gp043.pdf?expires=1394316180&id=id&accname=guest&checksum=6CDDD41F38A9E3520B7D632D09643DF0.

de decenas de miles de millones de dispositivos conectados para el año 2025 no parece descabellada[3].

De ahí que resulte crítico impulsar la seguridad en las transacciones, tanto jurídica como tecnológica. Este impulso se logra con el compromiso y la acción de instituciones y empresas que incorporen procedimientos seguros, así como mediante la regulación adecuada de la protección del consumidor[4].

Entre otros aspectos, la caída de precios de cada eslabón de la cadena ha facilitado que, finalmente, llegue al consumidor el IoT. Esa tendencia de bajada de precios fue anticipada por la ley de Moore que expresa que el número de transistores en un circuito integrado se duplica cada 18 meses[5]. Así, el precio y el tamaño de los transistores se reduce tanto que pueden integrarse en los objetos cotidianos[6]. Esto hace que los fabricantes de tecnología aporten equipos, conectables entre sí, para comunicar «cualquier cosa»[7].

Una de las implicaciones ha sido el desarrollo de tecnologías de la información («TIC») que procesan y analizan «Big Data» relacionados con nuestro día a día. Esta aproximación se ha fusionado con los conceptos de omnipresencia computacional, centrados en trasladar la información e interacción de los dispositivos tradicionales al entorno físico. Es decir, la innovación nos lleva desde las tecnologías inteligentes a la denominada Internet industrial[8] y se convierte en un nuevo paradigma tecnológico de computación ubicua e hiperconectada, equiparable a una explosión cámbrica.

En esta nueva aproximación los objetos cotidianos se pueden descubrir, localizar y controlar desde Internet o mediante aplicaciones que hacen de objetos desconectados objetos que están en red. De este modo, la idea básica es una Internet de objetos cotidianos conectados, creando así la base de dos áreas de investigación primordiales[9]:

---

3 Van der Berg, R., *Building the «Internet of Things»,* Informe de la OECD, abril 2012, pág. 1, recuperado el 29 de marzo de 2014, en http://www.internationaltransportforum.org/jtrc/PolicyBriefs/PDFs/2012-04-04.pdf.

4 Artículo 51.1 de la CE.

5 Moore, G., E. (1965), *Cramming more components onto integrated circuits*, Electronics, Vol. 38, p. 114-117.

6 Vide Brynjolfsson, E., McAfee, A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, Norton, New York, págs. 39-56.

7 Mattern, F. (2001), *Visión y fundamentos técnicos de la «Computación Ubicua»*, Novática, nº 153, p. 151-156.

8 Annunziata, M. (2013), *Welcome to the age of the industrial internet*, TED@BCG San Francisco, California, recuperado el 14 de diciembre de 2013, en http://www.ted.com/talks/marco_annunziata_welcome_to_the_age_of_the_industrial_internet.

9 Haya Coll, P., A., Montoro Manrique, G., Schnelle-Walka, D. *Op. Cit.*

- Comunicación máquina-máquina.
- Comunicación máquina-hombre y hombre-máquina

La expansión de los procesadores conectados sin cable hace posible la omnipresencia de la computación ubicua, que está en cualquier parte y en cualquier dispositivo por familiar que nos sea[10]. Con el uso de diminutos sensores, la vida se inunda de una capacidad nueva de procesar información y de efectuar las labores de comunicación de la información allá donde se encuentren.

En el futuro escenario, sería tan fácil comunicarse con un aparato como lo es en la actualidad con una persona, y no solo para el propietario del aparato, sino también para los servicios relacionados con ese aparato. Lógicamente, a la vez se abren varios debates, entre otros, respecto a la privacidad –de las personas y sus objetos–[11], seguridad informática[12], y protección de los consumidores.

No sólo desde la óptica del derecho, el fenómeno del IoT genera algunas dudas e incertidumbres, motivadas en gran medida por un cierta percepción de que la regulación vigente no resuelve de manera adecuada los conflictos potenciales o cuestiones planteados por las TIC, o lo que es lo mismo, que adolece de omisiones o lagunas en el tratamiento de tales cuestiones, en particular, a nivel de aplicación del derecho.

En este sentido, se impone una primera consideración de base, que, paradójicamente, tiene que ver con la afirmación de la inexistencia de lagunas en el ordenamiento jurídico. Esto es, la Ley puede presentar carencias u omisiones, sobre todo en casos, como el presente, en que irrumpen nuevos fenómenos sociales. Sin embargo, el ordenamiento jurídico no admite lagunas, y así se proclama por la regulación general de sistema de fuentes, que establece que las fuentes del ordenamiento jurídico son la ley, la costumbre y los principios generales del derecho como normas e cierre del sistema; normas o fuentes supletorias que, ante ausencias u omisiones en la regulación positiva, deben permitir la resolución de cualquier conflicto jurídico[13]. Es decir, el ordenamiento debe ofrecer en todo caso una solución incluso ante lagunas en la Ley; y de ahí deriva precisamente el deber de fallar o resolver que se impone en todo caso

10 Kellly, K (2007), *the next 5000 days of the web*, EG 2007, Monterey, California, recuperado el 14 de diciembre de 2013, en http://www.ted.com/talks/kevin_kelly_on_the_next_5_000_days_of_the_web.

11 El Parlamento europeo defiende la privacidad de los usuarios de tecnologías RFID, recuperado el 18 de diciembre de 2013, en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100614IPR76044+0+DOC+XML+V0//ES.

12 Scheneier, B. (2014), *The Internet of Things Is Wildly Insecure – And Often Unpatchable*, Wired, recuperado el 5 de marzo de 2014, en http://www.wired.com/opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

13 Art. 1 C.c.

a los Jueces y Tribunales, sin que puedan invocar para no hacerlo la inexistencia de laguna legal[14].

Lógicamente, la existencia de este principio de complitud que se predica del ordenamiento jurídico en su conjunto no impide que pueda apreciarse, sobre todo en sectores especialmente dinámicos como es el de las TIC, un anacronismo o falta de adaptación de la regulación legal vigente en un momento dado; y esta necesidad es palpable en ciertos aspectos que afectan a la transmisión de información y prestación de servicios a través de Internet. Pero también es cierto que la extensa regulación legal dictada en relación con los diversos ámbitos de actividad y de la vida social ofrece en muchos casos no sólo normas expresas, sino también principios generales informadores de los distintos campos normativos, que permiten dar solución a las dudas o conflictos que pueda plantear el desarrollo tecnológico.

Con el transcurso del tiempo desde los orígenes del comercio electrónico, los jueces y legisladores han podido desarrollar una mayor receptividad a tales cuestiones. Aunque ya se han desarrollado muchas tecnologías, proyectos y sistemas, dentro de la intersección de la protección de los consumidores y el IoT quedan todavía aspectos que deben ser abordados con mayor detenimiento como la complejidad del marco legal y tecnológico o la competencia digital[15].

Esta comunicación proporciona una visión general de la protección de los consumidores en ámbito del IoT. Una cuestión que, al igual que sucede en cualquier rama de la tecnología, es mucho más compleja y multidisciplinar de lo que la deformación unidimensional tiende a presentar. Para ello describiremos brevemente, desde una perspectiva socio-tecnológica, las facetas más relevantes de la protección de los consumidores respecto al IoT. Finalmente, se formulan las conclusiones de la presente comunicación.

2. IOT

2.1. Ecosistema

IoT es una tecnología y un desarrollo de mercado basada en la interconexión de los objetos cotidianos entre ellos y aplicaciones, cuyo potencial reside en la capacidad para combinar datos con personas, procesos y objetos. El IoT permitirá un ecosistema de aplicaciones y servicios inteligentes, a partir de sensores, redes avanzadas de comu-

14 Art. 7 C.c.

15 *Vide* la consulta pública con fecha 11 de diciembre de 2013 de la FTC, recuperado el 12 de diciembre de 2013, en http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop.

nicaciones y procesos analíticos basados en el big data[16]. Los dispositivos tendrán más patrones propios de comunicación y sus propias redes sociales, que podrán usar para compartir y agregar información, y realizar un control y activación automático. Los seres humanos vivirán cada vez más en un mundo donde las decisiones son tomadas por un grupo activo de aparatos tecnológicos capaces de interactuar entre sí.

Como se ha apuntado previamente, el IoT se basa en sensores, en redes de comunicaciones y en una inteligencia artificial que maneja todo el proceso y los datos que se generan[17]. Los sensores son los sentidos del sistema y, para que puedan ser empleados de forma masiva, deben tener bajo consumo y coste, un reducido tamaño y una gran flexibilidad para su uso en todo tipo de circunstancias. La evolución de Internet también precisa de potentes y seguras redes de comunicación inalámbrica Máquina a Máquina («M2M»), que hagan posible la incorporación a las redes y a los sistemas de objetos totalmente fuera de ellos hasta hace poco. Asimismo, es necesario aplicar inteligencia a los sistemas y a los objetos, aprovechando los datos recogidos por los sensores, para procesarlos y convertirlos en información útil y en actuaciones. Aquí las técnicas de análisis asociadas al «big data» son vitales. En ocasiones hay que aplicar potentes sistemas de información y de software avanzado que hagan posible el tratamiento de volúmenes de datos de una naturaleza variada y a gran velocidad[18].

2.2. Aplicaciones

Es la evolución de un primer Internet más centrado en las personas y cuyo potencial reside en la capacidad para combinar datos con personas, procesos y objetos. Los avances en integración y miniaturización de componentes y micro-sistemas, así como la creciente autonomía y flexibilidad de los robots de servicio está acelerando la difusión de sistemas embebidos en todo tipo de objetos físicos y artefactos desde ropa e incluso cuerpos humanos a casas, vehículos y sistemas de transporte, así como espacios públicos y ciudades. En estos y otros campos es posible encontrar también supuestos muy concretos de aplicación, como el marketing y la publicidad, en los que las nuevas posibilidades alcanzan rendimientos máximos.

Por otro lado, el IoT ya ha mostrado signos de revolucionar la manera como los minoristas interactúan con sus clientes cuando se trata de análisis en tiempo real y promociones. Aquí es donde «big data» y el IoT convergen, y las posibilidades son prácticamente infinitas. Mediante la combinación de dispositivos conectados, así como con los

16 Boyd, D., Crawford, K. (2011), *Six Provocations for Big Data. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, recuperado el 11 de enero de 2014, en http://ssrn.com/abstract=1926431.

17 Vide Brynjolfsson, E., McAfee, A. Ob. Cit., págs. 89-96.

18 White, T. (2012), *Hadoop: The Definitive Guide*, O'Reilly Media, 3ª Edición, Sebastopol.

datos agregados de los clientes, los minoristas pueden adaptar promociones y experiencias personalizadas para los clientes.

En muchos sentidos, el IoT permitirá a los minoristas de tipo tradicional disponer del tipo de información de los clientes en tiempo real que los minoristas de Internet siempre tuvieron. Es decir, una gestión menos expuesta a la incertidumbre en determinadas áreas. Estimar la demanda y adecuarla a la oferta será un ejercicio menos aventurado. La accesibilidad a la información acerca del comportamiento de los consumidores y el seguimiento puntual de sus patrones de compra puede contribuir a una estimación más fiel de su demanda, e incluso permitir la segregación de mercados y discriminación perfecta de precios. Las preferencias de los consumidores dejarán de ser la variable más difícil de aprehender en la demanda potencial de un producto y pasa a ser objeto de captura en aquellos bienes o servicios más ajustados a las posibilidades comerciales que ofrece las red, mediante la interlocución particularizada con los consumidores[19].

El IoT tiene el potencial de optimizar el proceso de compra y, al mismo tiempo, ofrecer un amplio elenco de opciones y una mayor personalización. Así, mediante el IoT y análisis inteligentes, es muy posible encontrarnos ante un escenario en el que los clientes entran en una tienda y sean guiados directamente a sus productos favoritos utilizando variables tales como historiales de búsqueda en línea, los flujos de datos que provienen de los dispositivos del cliente o su histórico de compras. Podemos decir que este escenario mejora sustancialmente la experiencia de compra del consumidor, pero genera suspicacias en términos de promociones en venta, protección de datos o publicidad engañosa[20].

2.3. Políticas

La generación de un clima de confianza e innovación responsable parece fundamental[21], si consideramos que el desarrollo del IoT tiene implicaciones a nivel de seguridad, privacidad y confianza[22]. Dichas políticas deben tener en cuenta la evolución tecnológica y la gestión del cambio. Asimismo, al mismo tiempo que el IoT se extiende a la

19 Ontiveros, E. (2001), *La economía en la red*, Taurus digital, Madrid, p. 85-86.

20 Los arts. 4 y 5 de la Ley General de Publicidad castigan la publicidad engañosa.

21 *Verbi gratia*, en 2011 se estimó que se producían 1632 millones de incidencias por año asociadas a una pérdidas financieras netas anuales por valor de 27.005 millones de Euros. Fuente: Europe Economics (2011), *Digital Content Services for Consumers: Assessment of Problems Experienced by Consumers (Lot 1) Report 4: Final Report*, Londres, recuperado el 15 de diciembre, en http://ec.europa.eu/justice/consumer-marketing/files/empirical_report_final_-_2011-06-15.pdf.

22 *Vide* las conclusiones de la consulta pública de la Comisión acerca del IoT, recuperado el 22 de diciembre de 2014, en http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.

vida cotidiana de las personas, se requiere identificar aquellas políticas o requerimientos regulatorios[23], cuyo impacto pueda ser previsto, así como en términos de información y educación[24] que son aspectos clave para el éxito del IoT.

3. ANÁLISIS ESPECÍFICO DE LAS CUESTIONES SUSCITADAS POR LOS CONTRATOS DE ADHESIÓN CON CONSUMIDORES EN EL IOT

Si bien la integridad de los datos y la privacidad son dos de las mayores preocupaciones cuando se habla del IoT, como se ha apuntado previamente, en esta comunicación se abordan los aspectos de la protección legal de los consumidores en la contratación en IoT. Recorremos dicho análisis a partir del punto de partida de cómo se puede proteger al consumidor en un contexto de las condiciones generales de contratación («CGC») en el IoT.

3.1. Validez del contrato de consumo

La principal cuestión legal referida a las CGC se refiere a la validez de las mismas. Este interrogante legal se mantiene como la cuestión más trascendente tanto en el ámbito de contratación real como virtual. La función espuria de las CGC permite al empresario predisponerte, ocupar un lugar preponderante en la relación negocial, todo por vía de la inclusión de las denominadas cláusulas abusivas.

Es decir, que al lado de las que podríamos denominar funciones justificadas de esta forma negocial, aparecen las funciones encubiertas que carecen de fundamentación en los principios elementales del derecho de los contratos: la buena fe y la equidad. Y si bien, este fenómeno de las CGC ha sido visto por la doctrina como un quiebro a los cánones clásicos en materia de contratos, sobre todo desde el punto de vista de la autonomía de la voluntad y las limitaciones a la libertad de fijar el contenido del acuerdo, ello no es óbice para desconocer los principios en los que descansa toda la estructura del Derecho y que tienden naturalmente a la reestructuración de las relaciones haciéndolas más justas y parejas.

---

23 La Comunicación de la Comisión sobre «la Internet de los Objetos» que esboza un marco de políticas públicas identifica un plan de acción centrado en la gobernanza, la privacidad y la protección de datos personales, la seguridad, el silencio de los chips, y la conciencia global institucional. Comunicación de la Comisión al Parlamento Europeo, de 18 de junio de 2009, denominada «Internet de los objetos: un plan de acción para Europa» [COM (2009) 278 final – no publicada en el Diario Oficial], recuperada el 9 de diciembre de 2013, en http://eur-lex.europa.eu/legal-content/ES/ALL/;jsessionid=qRwXTQcZsRsjTT6hB1rr7QsDjGyxP35vgMNtNTy1p3Gp16TygnnS!1365073497?uri=CELEX:52009DC0278.

24 Artículo 51.2 de la CE.

En este sentido, el contrato celebrado por medios electrónicos, se trata de un contrato de consumo, que deberá ser interpretado conforme a las normas de la ley de protección al consumidor (a favor del consumidor); si es un contrato con cláusulas predispuestas, en contra del predisponerte y a favor del adherente: y si es un contrato paritario, conforme al principio general de la buena fe[25].

Ello no es óbice para que las CGC entre profesionales puedan declararse nulas cuando sean contrarias a la buena fe y cause un desequilibrio importante entre los derechos y obligaciones de las partes, incluso aunque se trate de contratos entre profesionales o empresarios. Pero se habrá de tener en cuenta en cada caso las características específicas de la contratación entre empresas[26].

3.2. Eficacia jurídica de la contratación

A pesar del cambio de medio para la contratación, el fundamento de la contratación electrónica se encuentra en las normas que regulan la contratación tradicional, a través de la concurrencia de la oferta y de la aceptación establecidas en nuestro Código Civil[27] y Código de Comercio[28]. El cambio producido se refiere a que el medio para la emisión de las declaraciones de voluntad que perfeccionan todo contrato está basado en medios tecnológicos nuevos como las aplicaciones o agentes inteligentes. Por tanto, se incrementa la rapidez y fluidez en las transacciones, y se produce una relación coste-beneficio que favorece su expansión.

Históricamente, el reconocimiento de la eficacia jurídica de los contratos electrónicos se produjo en España a través de la jurisprudencia del Tribunal Supremo[29], para después ser objeto de tratamiento parcial en algunas leyes[30]. En la actualidad, la Directiva 2000/31/CE sobre comercio electrónico establece la obligación de los estados miembros de velar para que sus legislaciones permitan los contratos suscritos por vía electrónica y garanticen su eficacia y validez jurídica.

Asimismo, la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico («LSSI») declara la plena validez legal y eficacia de estos contratos[31], y su adecuación para cumplir con el requisito de la forma escrita a efectos probatorios si

25 Art. 1258 C.c.

26 Exposición de motivos de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.

27 Art. 1262 C.c.

28 Art. 54 C.C.

29 Al amparo del principio de libertad de forma.

30 Véase el artículo 5.3 de la Ley 7/1998, sobre condiciones generales de la contratación.

31 Art. 23 de la LSSI.

concurren determinadas condiciones. Evidentemente, con relación a la eficacia legal de los contratos electrónicos, se deberá tener en cuenta lo que dispone la regulación la firma electrónica[32]. Finalmente, hay que apuntar que hay negocios que por la trascendencia de su objeto se considera que no pueden celebrarse por vía electrónica[33].

No obstante, el desarrollo del comercio electrónico en el IoT plantea importantes riesgos para los consumidores. Entre otros, la posibilidad de enviar pedidos mediante agentes inteligentes[34], así como interfaces de compra que faciliten declaraciones negociales impulsivas o inconscientes; la posible falta de solvencia de la contraparte en la medida en que se contrata con su establecimiento virtual; y el empleo generalizado de CGC o permisos de aplicaciones abusivos.

3.3. Inseguridad jurídica

Los diversos actores del IoT han de poder contar con un marco jurídico que les permita confiar en una adecuada protección de sus legítimos derechos y expectativas en un grado al menos no inferior a la protección de que disponen en el comercio tradicional.

Por otra parte, entendemos que se debe reflexionar sobre la manera de probar en que podrá considerarse consumada la celebración de un contrato mediante aplicaciones o agentes inteligentes celebrado en IoT que pueda ser dotado de validez. Ya que tales contratos no hacen, en principio, uso de firmas electrónicas. La firma electrónica es la herramienta que permite, *inter alia*, determinar de forma fiable si las partes que intervienen en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

No obstante, el uso de la firma electrónica avanzada[35] o reconocida en la contratación electrónica es meramente voluntaria para las partes. La Ley 59/2003, de 19 de diciembre de firma electrónica, tan sólo atribuye a la firma electrónica reconocida[36], siempre que este basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, el mismo valor jurídico que la firma manuscrita con relación a los consignados en soporte papel.

---

32 En este sentido, favorecerá la implantación de la firma electrónica la reciente aprobación del Reglamento comunitario que sustituye a la Directiva de firma electrónica y que regula la identificación electrónica, recuperado el 12 de marzo, en http://europa.eu/rapid/press-release_MEMO-14-151_en.htm.

33 Art. 23.4 de la LSSI.

34 Véase el número especial dedicado a los agentes electrónicos del International Journal of Law and Information Technology, Vol. 9, núm. 3, otoño de 2001.

35 Art. 3.2 Ley de Firma Electrónica.

36 Art. 3.3 Ley de Firma Electrónica.

3.4. Falta de consciencia procesal

En algunos casos los menores pueden actuar por su cuenta y riesgo sin el consentimiento de sus padres; en otros casos, esta circunstancia puede afectar a los usuarios en general, que o no son conscientes de los modelos de negocio y transacciones subyacentes al IoT mediante aplicaciones o agentes inteligentes[37], o desconocen completamente las ramificaciones tecnológicas del IoT.

Incluso en los supuestos en que se aplique el consentimiento general, los jueces deben proceder al escrutinio del entorno del IoT en búsqueda de procesos y CGC abusivas, tal como sucede en el entorno en papel. Los jueces no pueden asumir automáticamente que las nuevas herramientas disponibles para los consumidores electrónicos serán suficientes contra la explotación. Asimismo, aunque el contexto del IoT pueda eliminar presiones sociales sobre los consumidores, genera, sin embargo, potenciales nuevos abusos por parte de las empresas. Por ello, la trascendencia de la supervisión judicial seguirá vigente.

No obstante, los jueces familiarizados con la peculiar naturaleza del entorno del comercio electrónico deberán afinar su escrutinio de los contratos electrónicos en el IoT. En particular, respecto a los nuevos tipos de procedimientos abusivos disponibles en el IoT. Como hemos comentado previamente, el entorno del IoT ofrece a las plataformas de comercio electrónico informaciones y datos de los consumidores que permiten dicho abuso. En primer lugar, el IoT permite la monitorización de multitud de datos y metadatos[38] de los usuarios, así como la fácil configuración de nuevos métodos de marketing y presentación.

En segundo lugar, las plataformas de comercio electrónico son capaces de identificar y ofrecer diferentes CGC de forma individualizada según el perfil del contratante[39]. Los jueces deben presumir que los negocios que practiquen este método, explotan a los consumidores, minando la presunción de aceptación válida del contrato.

---

37 El IoT creará 1,9 billones de dólares de valor económico. *Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets*, 11 de noviembre de 2013, recuperado el 15 de diciembre de 2013, en https://www.gartner.com/newsroom/id/2621015.

38 NISO (2010), *Understanding Metadata*, NISO Press, recuperado el 11 de diciembre de 2013, en http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

39 Esta práctica difiere claramente de aquellas técnicas legítimas de discriminación de precios, en las que las empresas identifican a los consumidores que adquieren más bienes o servicios que la mayoría. Véase Shwartz, A., Wilde, L., L. (1979), *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, Pennsilvania Law Review 127, enero, p. 630-682.

4. FUNDACIONES SÓLIDAS DE LA PROTECCIÓN DE LOS CONSUMIDORES

La protección de los consumidores es mucho más compleja y multidisciplinar que su marco jurídico. Para ello describiremos, desde una perspectiva multidisciplinar, las facetas más relevantes de la protección de los consumidores en el IoT. Es decir, la socio-económica, la cultural, la ético-legal, la política, y la tecnológica, todas ellas interconectadas entre sí.

4.1. Ámbito socio-económico

Internet es un contexto favorable para el desarrollo de iniciativas de autorregulación empresarial, dato que se trata de un área dinámica y en constante evolución que requiere una regulación flexible, donde la iniciativa privada cuenta con una gran pujanza y concurre además una particular sensibilización sobre la conveniencia de dotarse de modelos de actuación adecuados que incrementen la confianza de los usuarios.

En este sentido, tanto la LSSI como la Directiva 2000/31/CE relativa a los servicios de la sociedad de la información, han reconocido el valor de los Códigos de conducta como instrumento de ordenación del sector y complemento de los principios y normas jurídicas. De manera particular, la Ley 34/2002 encomienda a las Administraciones Públicas la labor de incentivar la elaboración y aplicación de los citados Códigos[40]. Al objeto de materializar ese mandato contenido en la Ley 34/2002, las Administraciones Públicas promueven, entre otras, la difusión y más amplio conocimiento de las iniciativas de establecimiento de sistemas de autorregulación relativos a la prestación de servicios de la sociedad de la información y al comercio electrónico[41].

Puede parecer una obviedad pero la mejor protección de los consumidores es la que ellos mismos se pueden procurar. A modo de ejemplo, las tiendas de aplicaciones permiten la retroalimentación e incentivan la valoración de las aplicaciones. Las clasificaciones de aplicaciones en las plataformas de aplicaciones son el resultado de un sistema complejo que contempla diversos factores, pero las metodologías necesitan ser más transparentes para el beneficio de usuarios y desarrolladores[42].

---

40 Art. 18.

41 En este ámbito, el «distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico», cuya regulación se encuentra establecida en el RD 1163/2005, y que constituye un importante mecanismo público de impulso de la autorregulación en este ámbito. Dicho RD establece los requisitos y el procedimiento de concesión de dicho distintivo.

42 Grupo de trabajo del Artículo 29, Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, recuperado el 11 de marzo de 2014, en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf.

Entre otros aspectos las clasificaciones deben facilitar información relevante y objetiva respecto a la metodología de clasificación, al objeto de facilitar métricas fiables para la toma de decisiones de los consumidores. Incrementándose la importancia de que las clasificaciones y la participación de los usuarios finales en las valoraciones reflejen los productos actuales y servicios ofrecidos, en particular si los gobiernos favorecen la opción de fomentar la autorregulación en el ecosistema del IoT.

4.2. Ámbito cultural

Desde la Declaración de los Derechos del Hombre y del Ciudadano, fruto de la Revolución Francesa de finales del siglo XVIII, la alfabetización total de la población pasó a constituir un objetivo universal de los poderes públicos[43]. Tres siglos después, este objetivo se ha cumplido casi totalmente en los países desarrollados, que han conseguido además que porcentajes significativos de sus ciudadanos alcancen niveles educativos universitarios. Ahora bien, una de las principales carencias actuales de la alfabetización en no pocos de esos países, es que no contempla la formación en competencias digitales, que, sin embargo, son decisivos para el desarrollo humano y laboral de los ciudadanos en la sociedad red.

En ausencia de una alfabetización digital integrada de forma equilibrada en los planes de enseñanza a todos los niveles, dicha alfabetización cede a la improvisación y al impulso de los factores comerciales. El usuario medio aprende por sí mismo, sin método y de forma descontextualizada, generándose indefensión ante el carácter pervasivo de la publicidad comportamental. Frente a ello, una de las áreas clave donde las políticas educativas pueden focalizarse es en la educación de competencias digitales y programación informática como parte de la educación secundaria y terciaria.

4.3. Ámbito ético-legal

La ética y la Ley son elementos fundamentales para el progreso de cualquier colectividad humana desarrollada y, sin embargo, en lo que se refiere a la tecnología, nos encontramos con que el rápido avance de estas ramas del saber provoca que, por un lado, colectividades e individuos tengan dificultades para establecer pautas éticas permanentes sobre su diseño, uso y aplicación, y, por otro, la legislación vaya a remolque de sucesivas innovaciones disruptivas[44].

No obstante, hay que precisar que si bien el marco legal y normativo de la protección a los consumidores, en líneas generales, es suficientemente flexible a priori para hacer frente eficazmente a las cuestiones que presenta el IoT. Lo que resulta más pro-

43 Art. 26.1 de la Declaración Universal de Derechos Humanos.

44 *Verbi gratia*, la introducción del mpeg Layer 3, más conocido como el mp3.

blemático es la estructura institucional y orgánica de la administración competente que requiere su modernización y un enfoque multidisciplinar que aborde los aspectos tecnológicos y económicos además de los legales.

Esta faceta de la protección de los consumidores, más allá de la aplicación del marco normativo y orgánico de la protección de consumidores al IoT, requiere una legislación internacional que proteja los legítimos derechos e intereses de personas físicas y jurídicas pues una legislación de carácter meramente nacional es insuficiente para generar la confianza de los consumidores y para proteger sus derechos y libertades de forma efectiva.

En el contexto actual[45], parece improbable que el consumidor medio sea un usuario informado y esté familiarizado con la contratación mediante dispositivos o aplicaciones informáticas, agentes inteligentes o M2M. Por ello, responsabilizarlos por actos imprevistos de los agentes puede ser injusto, y contraproducente. Por tanto, el régimen legal de la protección de los consumidores debe proteger específicamente a los consumidores en ámbito de contratación mediante aplicaciones informáticas, agentes inteligentes o M2M, en particular respecto a la exclusión de la responsabilidad de los desarrolladores, revendedores, y comerciantes *online*[46]. La modernización del marco jurídico de los servicios debe inscribirse con el compromiso contraído por la Comisión con objeto de «legislar mejor»[47].

Para fomentar la confianza de los usuarios en el IoT, debe incrementarse la transparencia en las relaciones con los prestadores de servicios, estableciéndose a cargo de éstos varias obligaciones de información inteligible, de manera que los consumidores puedan saber de forma accesible con quién contratan, a qué se obligan y qué medios de reclamación tienen a su disposición, así como respecto a la funcionalidad e interoperabilidad de los dispositivos y software; acceso a los productos y permisos de las aplicaciones, comportamiento autónomo y especificaciones de calidad del software; procesamiento de datos y comunicaciones comerciales vía electrónica.

4.4. Ámbito político

La ausencia o presencia de voluntad política a altos niveles es un factor diferencial y competitivo para el avance tecnológico. El caso de los EEUU es paradigmático, mientras que en muchos países de la UE esa voluntad política es mucho más débil o, como mínimo, menos evidente. Así, las Administraciones de EEUU han sido las más activas en

45 OECD (2013), *Protecting and Empowering Consumers in the Purchase of Digital Content Products*, OECD Digital Economy Papers, Núm. 219, OECD Publishing, recuperado el 21 de diciembre, en http://dx.doi.org/10.1787/5k49czlc7wd3-en.

46 Bain, M., Subirana, B. (2003), *E-commerce oriented software agents*, Computer Law & Security Report, Vol. 19, núm. 5, p. 384.

47 http://ec.europa.eu/enterprise/policies/smart-regulation/index_en.htm.

la apuesta por sectores estratégicos. Sobre todo aquellos relacionados con la innovación y las nuevas tecnologías. Entre las mismas, el desarrollo de la infraestructura y los protocolos que se convirtieron en Internet fueron financiados y desarrollados inicialmente con recursos del Estado[48].

En el campo de la seguridad jurídica en el ámbito digital las políticas públicas y las medidas legislativas y son de mayor importancia pues afectan a elementos esenciales de la construcción de confianza en los sistemas y redes como es el caso de la protección de los derechos de los consumidores.

4.5. Ámbito tecnológico

En la presente comunicación se plantea como hipótesis de trabajo la solución orientada a procesos. Ahora bien, ¿qué se entiende por proceso? Puesto que es habitual utilizar de manera indistinta la palabra proceso o procedimiento como si se tratara de los mismos conceptos, es conveniente ofrecer una definición de los mismos que ayude a su diferenciación.

4.5.1. Contextualización de las soluciones orientadas a procesos

Así, un proceso es una secuencia de actividades organizadas temporalmente, las cuales persiguen un objetivo o resultado concreto y que involucran en su desarrollo una serie de recursos tanto de carácter humano, como material y financiero, mientras que, por otra parte, un procedimiento es un conjunto de normas y de reglas que determinan la manera de proceder para conseguir un resultado. Mientras un proceso determina qué es lo que se hace, un procedimiento detalla cómo hacerlo.

La integración de objetos del mundo real en los procesos de negocio se está llevando a cabo de manera exitosa reduciendo la brecha entre medios, errores humanos y problemas de retraso de la información[49]. Se han obtenido muchos beneficios en términos económicos y de mejora de procesos[50]. Conseguir una mejor integración de los mundos

48 Beas, D., *El mito de la incompetencia del Estado*, El País, 10 de enero de 2014, recuperado el 11 de enero de 2014, en http://elpais.com/elpais/2013/12/08/opinion/1386534964_232781.html.

49 Strassner, M., Schoch, T. (2002), *Todays Impact of Ubiquitous Computing on Business Processes*. En Friedemman Mattern, Mahmoud Nagshineh editors, *Short Paper Proc. Of International Conference on Pervasive Computing*, p. 62-74.

50 Langheinrich, M., Coroama, V., Bohn, J., Rohs, M., *As we may live – Real-world implications of ubiquitous computing*, Technical report, Swiss Federal Institute of Technology, recuperado el 22 de febrero de 2014, en http://www.jjbohn.com/papers/langhein_aswemaylive_2002.pdf ; Fleisch, D., *Business perspectives on Ubiquitous Computing. Technical report*, M-Lab Working, Switzerland, recuperado el 22 de febrero de 2014, en http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.197.7612&rep=rep1&type=pdf.

virtuales y reales no sólo mejora los procesos de negocio sino que también facilita el desarrollo de nuevos modelos de negocio como la suscripción a cualquier objeto[51].

Sin embargo, abordar el desarrollo de este tipo de sistemas no es una tarea sencilla. Los procesos de negocio están cambiando constantemente, lo que a su vez requiere la evolución de los sistemas que los soportan. Además, los sistemas de software en el contexto del IoT involucran un amplio espectro de tecnologías para conseguir desarrollar la intersección entre los mundos físico y virtual[52]. Esta heterogeneidad obliga al desarrollador a conocer los detalles de cada una de las tecnologías necesarias para desarrollar el sistema, haciendo que estos sistemas sean difíciles de desarrollar y mantener.

El enfoque de solución orientada a procesos planteado, de forma análoga a la innovación de procesos[53], sigue una lógica, la cual se estructura en las etapas de análisis de situación, acción creativa, aplicación de procesos, medición de resultados y seguimiento de los mismos al objeto de ajustar su aplicación y mejorar sus efectos.

Lógicamente, las etapas descritas simplifican un proceso que incluso puede llegar a ser mucho más complejo, entre otras cosas por la consideración sistémica de la tecnología, en la que la modificación de una de las partes del mismo puede causar efectos inesperados en otras partes o elementos del sistema. Es decir, la solución orientada a procesos debe abordarse siempre de manera global, midiendo cada una de las repercusiones posibles.

4.5.2. Soluciones orientadas a procesos

Como punto de partida tomaríamos el requerimiento de la incorporación de normativa y obligaciones contractuales en las dinámicas de modelado de procesos de negocio, en particular respecto a la contratación mediante aplicaciones o agentes inteligentes. En este contexto, se pretende diseñar una interfaz de usuario amigable e intuitiva para

---

51 Zaz, D., *The Suscription Economy's Secret Weapon*, recuperado el 7 de febrero de 2014, en http://www.fastcompany.com/3024523/innovation-agents/the-subscription-economys-secret-weapon.

52 La confluencia de lo físico y lo virtual tiene el potencial de transformar desde productos, procesos de producción y modelos de negocio. En este sentido, O'Reilly, T., Stogdill, J. (2014), *Tim O'Reilly & Jim Stogdill Explore Software-Hardware-Everywhere*, recuperado el 15 de marzo en 2014, en https://www.youtube.com/watch?v=zhUEvsq1xOo&list=PLZ71VONYwuXP7k9DbWpr57OpkP4QBQ285.

53 «La innovación en procesos supone la puesta en marcha de métodos de producción nuevos o significativamente mejorados, así como la incorporación de nuevos métodos de provisión del producto o prestación del servicio. Esto puede conllevar la incorporación o cambios significativos en técnicas, equipamiento o software.» OCDE, Oslo Manual. *The measurement of scientific and technological activities proponed guidelines for collecting and interpreting technological innovation data*, recuperado el 9 de enero de 2014, en http://www.oecd.org/sti/inno/2367580.pdf.

el consumidor cuando se comunique con una máquina, un aplicación informática o su propio agente inteligente.

De acuerdo al artículo 18 de la LSSI, se sugiere la inclusión como procedimiento en los códigos de conducta sectoriales, del establecimiento de métricas para el diseño de algoritmos que determinasen la mejor adaptación de los procesos de negocio a la normativa de protección de los consumidores –extrapolándose las tres leyes de la robótica al software del IoT[54]-. Incluyéndose infografías[55] o diagramas de flujo de entrada/salida y procesamiento entre máquinas para su mejor comprensión por parte de los consumidores.

Esta opción sería aplicable análogamente a la sistematización de las «licencias de adhesión» Creative Commons[56] en el ámbito de los derechos de autor que se representan en tres niveles o capas que manifiestan en esencia el mismo mensaje pero escritas según diferentes códigos[57]:

- Legal
- Humano
- Máquina

Asimismo, los trabajos de estandarización de procesos y reglas en ámbito del comercio electrónico entre empresas, basado en el ebXML de las Naciones Unidas para definir el marco tecnológico a nivel mundial sobre el que el Extensible Markup Language («XML») puede ser normalizado, podría replicarse en el contexto del IoT, al objeto de establecer un marco global de adecuación a la normativa de protección de los consumidores en ámbito del IoT[58].

Entre otras medidas, el establecimiento de la certificación de procesos de acuerdo a los estándares legales por parte de terceros cualificados, incluyéndose aspectos de seguridad, privacidad y otras características de cualquier modelo de negocio, redundarían en un mejor marco regulatorio de protección a los consumidores. Ello podría implicar el uso de aplicaciones que se ejecutasen en los teléfonos móviles de los usuarios que apo-

54 El célebre autor Isaac Asimov escribió las tres leyes de la robótica hace más de medio siglo. Aparecidas por primera vez en el relato *Runaround* (1942), establecen que un robot debe dar la máxima prioridad a la protección de la vida humana, a la obediencia a las órdenes humanas, a su propia protección, en ese orden, obligatoriamente.

55 Infografía del IoT, recuperado el 21 de diciembre de 2013, en http://blogs.cisco.com/diversity/the-internet-of-things-infographic/.

56 https://creativecommons.org/.

57 Vide licencias CC, recuperado el 1 de diciembre de 2013, en https://creativecommons.org/licenses/.

58 En el mismo sentido respecto a la contratación mediante agentes inteligentes, Bain, M., Subirana, B., *Op Cit*., p. 385.

yasen a los consumidores en la toma de decisiones de la protección a los consumidores cuando se enfrentasen con objetos controlados por aplicaciones. Dichas aplicaciones se convertirían en intermediarios entre los derechos de los consumidores y las CGC de las comerciantes electrónicos, al objeto de buscar el punto de equilibrio e informar al consumidor del resultado de la intermediación para su consentimiento informado[59].

Esta práctica de la certificación de procesos en el contexto del IoT se sistematizaría sobre la base conceptual del artículo 25 de la LSSI. Dicho artículo regula los denominados terceros de confianza que en el ámbito del IoT y la contratación mediante agentes inteligentes ampliarían su ámbito de actuación a la certificación de las especificaciones legales de los modelos de negocio de las empresas implicadas de acuerdo a la normativa de protección de los consumidores y contratos de consumo[60].

Otro de los elementos relevantes que la solución orientada a procesos evidencia es la repercusión organizacional que representa, medida desde el punto de vista del recurso humano. Cualquier cambio y más cuando se trata de un cambio tecnológico, es habitualmente visto como una amenaza y provoca resistencias. Por tanto, se debe ejercer una importante tarea de liderazgo que logre implicar a los consumidores y empresas y pueda construir estructuras más robustas basadas en la participación de todos los implicados.

5. CONCLUSIONES

La manera en que las políticas y tendencias regulatorias resuelvan la protección jurídica de los consumidores, afectará de manera decisiva a la economía de Internet. En cualquier caso, el incremento de la seguridad jurídica en el IoT, resulta crítico para la creación de la estabilidad en la conducción de las transacciones electrónicas y ayudará a facilitar el desarrollo tecnológico.

El nuevo escenario plantea dudas legítimas respecto a la posible inadecuación del régimen legal de y aplicación administrativa de la protección de los consumidores. En particular, se incrementan las posibilidades de que las empresas puedan explotar nuevos métodos de negocio que permitan técnicas abusivas para con los consumidores. Por otro lado, las empresas insisten en que la regulación de protección al consumidor no sea

59 Una aplicación similar ha sido previamente desarrollada. Vide Broenink, G., Hoepman, J.H., van't Hof, C., van Kranenburg, R., Wisman, T. (2011), *The Privacy Coach: supporting customer privacy in the Internet of things*. TNO, recuperado el 11 de diciembre, en http://arxiv.org/abs/1001.4459.

60 Los terceros de confianza son una tercera parte, con reconocimiento de las dos partes implicadas, que se encargará de archivar las declaraciones de voluntad que integran los contratos electrónicos y que consigna la fecha y la hora en que dichas comunicaciones han tenido lugar.

excesiva al objeto de no impedir el éxito de los nuevos modelos de negocio que la tercera revolución digital puede generar.

Finalmente, la revolución tecnológica de la que somos testigos excepcionales en los últimos años ha provocado un cambio radical en nuestra sociedad. Lo expuesto adquiere una mayor dimensión en el IoT, pues según su propio nombre indica cualquier movimiento regulatorio, político o empresarial, afectará potencialmente a millones de consumidores extendiéndose sus efectos con carácter transversal a la práctica totalidad de sectores económicos y sociales implicados.

COMUNICACIONES SOBRE CIBERCRIMINALIDAD

SEXTING Y VICTIMIZACIÓN SEXUAL ONLINE: PREVALENCIA Y FACTORES DE RIESGO ENTRE ADULTOS[1]

Manuel Gámez-Guadix
Erika Borrajo
Esther Calvete
Universidad de Deusto

Carmen Almendros
Universidad Autónoma de Madrid

RESUMEN: El sexting (i.e., el intercambio de contenidos sexuales sobre uno mismo a través de medios electrónicos) y la victimización sexual online (VSO) representan dos fenómenos interpersonales en auge que han sido escasamente estudiados entre adultos. La victimización sexual en diferentes contextos, tales como el trabajo, la pareja, o el colegio, es un reconocido problema social de gran importancia por su alta prevalencia y por sus consecuencias negativas. En los últimos años, la victimización sexual ha comenzado también a manifestarse a través de las nuevas tecnologías, en fenómenos tales como el grooming o el cyberbullying de carácter sexual. Sin embargo, poco se ha investigado hasta la fecha sobre los factores de riesgo para la VSO. Este estudio tuvo dos objetivos principales: 1) explorar la ocurrencia de sexting y VSO entre adultos en función del sexo, la edad y la orientación sexual; y 2) analizar si participar en sexting constituye un factor de riesgo para sufrir VSO. La muestra de este estudio estuvo compuesta por 873 adultos españoles entre 18 y 60 años (65,4% mujeres). Los resultados mostraron que aproximadamente dos de cada tres adultos había participado en sexting y uno de cada tres había experimentado VSO. En general, no se encontraron diferencias en sexting entre varones y mujeres; sin embargo, el sexting fue más frecuente entre adultos jóvenes y entre no-heterosexuales. La VSO, por su parte, fue más frecuente entre las mujeres, entre adultos jóvenes y de mediana edad (< 45 y.o.) y entre los no-heterosexuales. Por último, los hallazgos mostraron que participar en sexting incrementó la probabilidad de sufrir VSO tras controlar el efecto del sexo, la edad y la orientación sexual. Estos resultados tienen importantes implicaciones para la investigación futura en este campo y para la prevención de la victimización online. Palabras clave: Sexting; sexual victimization; nuevas tecnologías; Internet; conductas sexuales.

PALABRAS CLAVE: Falten les paraules clau.

Internet ha revolucionado muchos aspectos de las relaciones interpersonales, incluyendo el desarrollo de nuevas formas de comunicación íntima y de interacción sexual

1 Esta investigación ha sido financiada por el proyecto concedido a Manuel Gámez-Guadix por el Ministerio de Economía y Competitividad, Ref. PSI2012-31550.

(Döring, 2009; Strassberg, McKinnon, Sustaíta y Rullo, 2013; Whittle, Hamilton-Giachritsis, Beech y Collings, 2012). En este contexto, el sexting (i.e., la creación y envío de contenidos sexuales a través de medios electrónicos) y la victimización sexual online (VSO) constituyen dos fenómenos interpersonales en auge relacionados con el uso de las nuevas tecnologías. En los últimos años, ambos han recibido creciente atención social y empírica, incrementándose la preocupación sobre su alcance y sus posibles consecuencias (Drouin, Vogel, Surbey y Stills, 2013; Mitchell, Finkelhor, Jones y Wolak, 2012; Mitchell, Wolak y Finkelhor, 2007; Reyns, Burek, Henson y Fisher, 2013). La prevalencia del sexting y de la VSO ha sido considerablemente estudiada entre adolescentes (Mitchell et al., 2012; Mitchell et al., 2007); por el contario, poco es sabido sobre la prevalencia y las formas en que se manifiestan entre adultos de mediana edad y mayores (Barak, 2005; Drouin et al., 2013). Asimismo, se ha señalado que el sexting podría constituir un comportamiento de riesgo asociado con diferentes problemas, tales como comportamientos sexuales de riesgo (e.g., relaciones sexuales sin protección; Benotsch, Snipes, Martin y Bull, 2012) o diferentes tipos de victimización no específicamente sexual (Reyns et al., 2013). Sin embargo, hasta la fecha, en nuestro conocimiento, ningún estudio previo ha analizado específicamente la relación entre el sexting y la VSO.

1. SEXTING: CARACTERÍSTICAS Y PREVALENCIA

El sexting ha sido generalmente definido como la creación y envío voluntario de textos, fotos o videos con un contenido sexual o erótico (e.g., mensajes de texto, fotografías, videos, etc.) a través de Internet o del móvil (e.g., vía mensajes, redes sociales, webcams, etc; Drouin et al., 2013; Gordon-Messer, Bauermeister, Grodzinski y Zimmerman, 2012; Mitchell et al., 2012). Los datos disponibles sugieren que el sexting es frecuente tanto entre adolescentes (e.g., Rice et al., 2012) como en adultos jóvenes (e.g., Benotsch et al., 2012). Además, el sexting parece producirse mayoritariamente en el contexto de una relación de pareja, pero no exclusivamente en ella. Así, en el estudio Sex and Tech (The National Campaign to Prevent Teen and Unplanned Pregnancy, 2008), se encontró que el 83% de las mujeres adultas jóvenes y el 75% de los hombres adultos jóvenes que han enviado contenido sexual dicen haber enviado dicho material a la pareja, el 21% de mujeres y el 30% de los hombres lo han hecho a alguien a quien querían en ese momento o con quien querían mantener una relación, y el 15% de las mujeres y el 23% de los hombres lo han hecho a alguien que sólo conocían online. De forma similar, Drouin et al. (2013) encontraron que la información escrita, fotos o videos sexuales eran enviados con mayor frecuencia a parejas con las que existía un compromiso, y no tanto a parejas sexuales casuales o con las que cometían infidelidades.

Sin embargo, poco es sabido sobre otras variables personales relacionadas con el sexting, como el sexo y la orientación sexual. Entre los escasos estudios sobre diferencias según sexo se ha encontrado que, en general, varones y mujeres adultos jóvenes se

implican con similar frecuencia en conductas relacionadas con el sexting (Benotsch et al., 2012; Reyns et al., 2013; Weisskirch y Delevi, 2011), aunque los hallazgos han sido mixtos (Baumgartner, Valkenburg y Peter, 2010). Respecto a la orientación sexual, el único estudio previo hasta nuestro conocimiento que informó sobre las diferencias en sexting entre adultos heterosexuales y no heterosexuales (homosexuales y bisexuales) no encontró diferencias significativas (Gordon-Messer et al., 2012).

La mayoría de los estudios se han llevado a cabo entre adultos jóvenes, principalmente estudiantes universitarios (Benotsch et al., 2012; Drouin et al., 2013), por lo que es escasa la evidencia empírica sobre el sexting entre adultos mayores (Wiederhold, 2011). La investigación parece haber asumido que el sexting entre adultos de mayor edad es considerablemente menos frecuente en comparación con los adolescentes y adultos jóvenes.

2. VICTIMIZACIÓN SEXUAL ONLINE (VSO)

La victimización sexual en diferentes contextos, tales como el trabajo, la pareja, o el colegio, es un reconocido problema social de gran importancia por su alta prevalencia y por sus consecuencias negativas a corto y largo plazo (Bramsen et al., 2013; Gámez-Guadix, Straus y Hershberger, 2011). En los últimos años, la victimización sexual ha comenzado también a manifestarse a través de las nuevas tecnologías. El estudio de fenómenos tales como el «grooming», o acoso sexual de un adulto a un menor (Wachs, Wolf y Pan, 2012), y el cyberbullying, o acoso entre iguales online, el cual también puede ser de tipo sexual (Calvete, Orue, Estevez, Villardón y Padilla, 2010; Gámez-Guadix, Orue, Smith y Calvete, 2013), han puesto de manifiesto que las agresiones y VSO de menores están lejos de ser poco frecuentes. La VSO entre adultos es otro tipo de victimización online que ha sido largamente descuidada a nivel empírico (Barak, 2005).

La VSO, como es definida en el presente estudio, incluye la experiencia de algún tipo de presión a través de Internet o el teléfono móvil para obtener cooperación o contacto sexual (e.g., compartir información sexual, enviar imágenes con contenido sexual, o hacer algo sexual a pesar de que la víctima no lo desea) así como la distribución o difusión por parte del perpetrador de imágenes o información sexual de la víctima en contra de la voluntad de esta. Son escasos los estudios que han evaluado la VSO a través de instrumentos con unas adecuadas propiedades psicométricas. La mayoría de las investigaciones han empleado dos o tres ítems para medir variables relacionadas como, por ejemplo, la solicitud sexual online no deseada (Baumgartner et al., 2010; Mitchell et al., 2007). Aunque estos estudios han aportado información preliminar de gran valor sobre las experiencias sexuales indeseadas online, es de gran importancia para el avance en este campo realizar un análisis más exhaustivo de las experiencias que constituyen VSO.

Como se ha mencionado, poco es sabido sobre la prevalencia de la VSO entre adultos. Entre los pocos estudios llevados a cabo, Goodson, McCormick y Evans (2001) encontraron en su muestra que el 15,8% de estudiantes universitarios (24.4% de las mujeres y el 8% de los varones), se habían sentido sexualmente acosados durante conversaciones online. Asimismo, Baumgartner et al. (2010) encontraron que el 4.6% de los hombres y el 6.7% de las mujeres se habían ofrecido sexualmente online en los últimos seis meses. Respecto a las diferencias en función del sexo, aunque la evidencia es escasa entre adultos, las mujeres parecen ser víctimas con mayor frecuencia que los varones (Baumgartner et al., 2010; Goodson et al., 2001). Esto es congruente con los datos de numerosos estudios que han encontrado que las mujeres sufren con mayor frecuencia la victimización sexual offline que los varones (Gámez-Guadix et al., 2011; Hines y Saudino, 2003). Al igual que en el caso del sexting, poco es sabido sobre la relación entre variables demográficas, tales como la edad o la orientación sexual, lo cual podría estar limitando las estrategias preventivas.

2.1. ¿Por qué analizar la relación entre el sexting y VSO?

Parece razonable pensar que el sexting constituya un factor de riesgo para la VSO. Como se ha mencionado, el sexting implica la creación y el envío de contenidos sexuales (información o imágenes sexuales) que podrían ser utilizados para chantajear a la víctima u ocasionarle un daño (p.ej. a través de su difusión). Además, las personas podrían ser más proclives a revelar online información sobre cuestiones íntimas y sexuales que a través de comunicaciones cara a cara (Wolak, Finkelhor, Mitchell e Ybarra, 2010). Por ello, es posible que el sexting constituya un comportamiento online que aumente la exposición de los participantes para sufrir VSO ante los posibles perpetradores. Una vez que el contenido sexual ha sido enviado, podría incrementarse el contacto entre la víctima y el perpetrador, pudiendo este contacto escalar hacia otros contactos no deseados entre ambos, tales como amenazas para recibir más contenidos sexuales o para un encuentro offline (Reyns et al., 2013). Por otro lado, las mismas características tecnológicas que permitieron el envío del contenido sexual, permiten el envío de este a terceras personas conocidas o desconocidas sin el consentimiento de la víctima (Reyns et al., 2013). Una vez enviado el material a través de medios electrónicos, este puede ser trasmitido en cualquier momento y en cualquier lugar (Smith, 2012), incrementando la probabilidad de la VSO y la dificultades de escapar de ella.

Sin embargo, los estudios disponibles sobre la asociación entre sexting y VSO son muy limitados. Como se señaló anteriormente, la victimización online es un problema emergente de gran importancia dada la elevada prevalencia y las posibles consecuencias perjudiciales en sus víctimas (por ejemplo, Mitchell, Ybarra y Finkelhor, 2007). Desde este punto de vista, los estudios que se centran en la aclaración de los factores de riesgo para VSO pueden ser de gran valor.

2.2. El presente estudio

Teniendo en cuenta la escasez de investigación sobre la ocurrencia del sexting y la VSO entre adultos de un amplio rango de edad, el primer objetivo del presente estudio consistió en explorar la prevalencia y manifestaciones de estos dos fenómenos, focalizándonos en el análisis de las diferencias en función del sexo, la edad y la orientación sexual, que hasta la fecha han sido escasamente estudiadas entre adultos. Un segundo objetivo consistió en analizar la relación entre el sexting y la probabilidad de la VSO. Con base a lo arriba expuesto, nosotros hipotetizamos que mayor implicación en sexting estará asociada con una mayor probabilidad de sufrir VSO.

2.3. Método

2.3.1. Participantes

La muestra de este estudio estuvo compuesta por 873 adultos españoles (65,4% mujeres). La recogida de la muestra fue llevada a cabo a través de una breve encuesta online. Los investigadores utilizaron sus clases y anuncios online en las redes sociales para pedir a los posibles participantes completar la encuesta anónima. Los participantes tenían edades comprendidas entre los 18 y los 60 años (M = 31.11; ST = 9.58). El 29.7% tenía entre 18 y 24 años, el 40.2% entre 25 y 34 años, el 18% entre 35 and 44 años, y el 12.1% entre 45 y 60 años. El 89.9% indicaron que eran heterosexuales, el 5.8% homosexuales y el 4.3% bisexuales.

Los investigadores solicitaron el consentimiento informado a los participantes, que fueron informados del objetivo general del estudio, de que su participación era voluntaria y anónima, y de que en cualquier momento podían sentirse libres de abandonar el estudio. No se les solicitó su nombre ni ningún otro dato que permitiera identificar las respuestas. Una vez que los participantes facilitaron el consentimiento, se les dio acceso a la encuesta. Inicialmente, 957 personas contestaron algún ítem. Los datos fueron revisados para detectar patrones de respuesta aleatorios y encuestas con un gran número de datos perdidos (i.e., más de la mitad de los ítems no respondidos). Setenta y cuatro participantes (8.78%) fueron excluidos por alguna de estas razones, obteniéndose la muestra final del estudio. El estudio fue revisado y aprobado por el Comité de ética en la investigación de la Universidad de Deusto.

2.3.2. Medidas

Cuestionario sociodemográfico. Incluimos preguntas referentes a la edad, el sexo, la orientación sexual, el nivel educativo y el lugar de residencia.

Sexting. Ante la ausencia de instrumentos validados previamente para medir este constructo, nosotros elaboramos una serie de preguntas con el objetivo de evaluar si los participantes se habían implicado en alguna ocasión en sexting. Para elaborar los ítems,

nosotros cruzamos dos niveles de contenidos («fotos, imágenes o videos con contenido erótico o sexual» e «información escrita o mensajes de texto») con tres posibles destinatarios (tu pareja, un amigo o conocido, y una persona solo conocida online). Así, obtuvimos 6 ítems. Para diferenciar las conductas de sexting del envío de fotos e información como consecuencia del acoso (e.g., tras recibir amenazas), pedimos a los participantes que indicasen cuántas veces habían llevado a cabo estas conductas *de manera voluntaria*, es decir, porque ellos querían o les apetecía. La escala de respuesta fue: 0 = *nunca*; 1 = *1 o 2 veces*; 2 = *3 o 4 veces*; 3 = *5 o 6 veces*; y 4 = *7 o más veces*. El coeficiente alpha de consistencia interna para la escala fue de .78.

Victimización sexual online. Dado que tampoco se dispone de instrumentos previos con unas adecuadas propiedades psicométricas para medir VSO, nosotros elaboramos un nuevo instrumento compuesto por 10 ítems para medirlo. Nosotros elaboramos ítems para medir dos niveles de victimización online (insistencia y amenazas), siguiendo la aproximación de medidas previas ampliamente empleadas para medir victimización sexual en contextos interpersonales (e.g., CTS2; Straus, Hamby, Boney-McCoy y Sugarman, 1996). Nosotros cruzamos estos dos niveles con las siguientes situaciones específicas de victimización: insistir/amenazar para obtener fotos o videos eróticos o sexuales, para revelar información sexual sobre ti, para llevar a cabo algún comportamiento sexual online (p.ej., a través de webcam), y para mantener relaciones sexuales offline (e.g., «Alguien te ha insistido online para que le envíes fotos o vídeos eróticos o sexuales a pesar de que tú no querías», «Alguien te ha amenazado online para que le envíes fotos, imágenes o vídeos con contenido erótico o sexual tuyo»). Además, incluimos 2 ítems adicionales para medir un tipo de victimización específico del contexto online, a saber: la difusión de información personal de la víctima en contra de su voluntad (e.g., «Alguien ha difundido o colgado en Internet fotos o vídeos con contenido erótico o sexual tuyo sin tu permiso»; Gámez-Guadix et al., 2013). El contenido específico de los ítems es incluido en la Tabla 2. Los participantes tenían que indicar cuántas veces habían sufrido en alguna ocasión cada uno de los tipos de VSO empleando la siguiente escala: 0 = *nunca*, 1 = *1 o 2 veces*; 2 = *3 o 4 veces*; 3 = *5 o 6 veces*; y 4 = *7 o más veces*. El coeficiente alpha de consistencia interna del cuestionario fue α = .81.

2.4. Resultados

2.4.1. Prevalencia del sexting

En la tabla 1 se presenta la prevalencia total de cada comportamiento de sexting analizado. Los datos mostraron que hasta el 66.8% de los participantes se implicaron en al menos un tipo de sexting. Los porcentajes de los comportamientos de sexting individuales oscilaron entre el 11.1% («envío de fotos, imágenes o videos a alguien que has conocido en internet pero que no conocías en persona») y el 58.3% («envío de información escrita con contenido erótico o sexual a tu pareja»). En general, la prevalencia

para el envío de material sexual a la pareja (60%) fue mayor que el envío a amigos o conocidos (27.9%) o a desconocidos/solo conocidos online (18.6%) ($\chi^2_{(2, N=873)}$= 357, p < .001). Asimismo, el sexting consistente en el envío de información escrita con contenido erótico o sexual fue más frecuente que el envío de fotos, imágenes o videos (65.4% and 33.8%, respectivamente; $\chi^2_{(1 , N=873)}$= 173, p < .001).

Respecto a las diferencias por sexo, no se encontraron diferencias entre varones y mujeres en la prevalencia total del sexting ($\chi^2_{(1 , N=873)}$ = .41, *ns*). No obstante, algunas diferencias emergieron cuando se tomó en cuenta el destinatario. Así, el sexting fue más frecuente entre los varones cuando la información escrita, imágenes o videos eran enviados a amigos o conocidos o a personas solo conocidas online; por el contrario, no hubo diferencias entre ambos cuando el contenido sexual era enviado a la pareja. El sexting fue también más frecuente entre los adultos de 19 a 24 años (70,5%) y entre 25 y 34 años (75,8%) que entre adultos de 35 a 44 años (63,6%) y de 45 a 60 años (33%) ($\chi^2_{(3 , N=873)}$ = 100.17, p < .001). Asimismo, más homosexuales y bisexuales (86,2%) que heterosexuales (64,4%) se implicaron en sexting ($\chi^2_{(1 , N=873)}$= 12.76, p < .001).

2.4.2. Prevalencia de la VSO

En la tabla 2 se presenta la prevalencia total para cada tipo de VSO. Los datos mostraron que el 37.5% de los participantes fueron víctimas de algún tipo de VSO. Los porcentajes de los comportamientos de VSO individuales oscilaron entre el 1.1% («alguien ha difundido o colgado en Internet fotos o videos con contenido erótico o sexual tuyo sin tu permiso») y el 28.2% («alguien te ha insistido para que le envíes videos eróticos o sexuales a pesar de que tú no querías»). La prevalencia de tipos relacionados con insistencia a pesar de que la víctima no quería (36.7%) fueron significativamente mayor que las amenazas (4.6%) y la difusión de contenidos sin el consentimiento de la víctima (3.7%) ($\chi^2_{(2, N=873)}$= 460, p < .001).

La VSO fue más frecuente entre mujeres que entre los varones (41.6% vs 31.9%; $\chi^2_{(1 , N=873)}$= 7.43, p < .01). La prevalencia de VSO fue también más frecuente entre los 19 y 24 años (39%), los 25- 34 años (43.1%), y los 35-44 (37.3%) que entre los adultos mayores (45-60 años) (21.4%; $\chi^2_{(3 , N=873)}$= 15.91, p < .01). Finalmente, más personas no heterosexuales (63.9%) que heterosexuales (35.5%) sufrieron VSO ($\chi^2_{(1 , N=873)}$= 18.41, p < .001).

2.4.3. Relación entre el sexting y el acoso sexual online

Finalmente, analizamos si participar en sexting incrementaba la probabilidad de sufrir VSO. Para ello estimamos un modelo de regresión logística en el que incluimos el sexting como variable predictora. Asimismo, para controlar su posible efecto sobre la VSO, incluimos como variables predictoras el sexo, la edad y la orientación sexual. La VSO fue dicotomizada (0 = *nunca*; 1= *haber sido víctima alguna vez*) y usada como

variable criterio. Los resultados de la regresión se presentan en la tabla 3. Como puede observarse, el sexting y la VSO mostraron una relación estadísticamente significativa (b = .77; p <.001). Concretamente, cada aumento de un punto en la escala de 5 puntos de sexting se asoció con el aumento de la probabilidad de VSO 2.16 veces (OR =2.16; 95% CI: 1.68-2.77; $p < .001$). Además, las mujeres (OR =2.22; 95% CI: 1.50-3.31; $p < .001$), los adultos jóvenes (OR = .98; 95% CI: .96-.99; $p < .05$) y los participantes no-heterosexuales (OR =2.60; 95% CI: 1.40-4.81; $p < .01$) fueron significativamente más propensos a sufrir VSO.

2.5. Discusión

La finalidad de este estudio consistió en incrementar la evidencia empírica sobre la ocurrencia y las características de dos fenómenos relacionados con las interacciones sexuales en Internet, a saber, el sexting y la VSO, así como la relación entre ambos. Los resultados pusieron de manifiesto que un elevado número de adultos (aproximadamente dos de cada tres) participó en conductas consideradas sexting and un considerable porcentaje también informó de algún tipo de VSO (un tercio de la muestra total). Además, los datos indicaron que el envío voluntario de contenidos sexuales (i.e., sexting) incrementa significativamente la probabilidad de sufrir VSO. Este es el primer estudio llevado a cabo hasta el momento que analizó e informó sobre la relación entre ambos fenómenos.

Los hallazgos indican que el sexting representa una forma habitual de relacionarse sexualmente a través de Internet. Aproximadamente, el 66% de los adultos reconocieron haber intercambiado algún contenido sexual online. Estos datos son consistentes con los de estudios previos entre adultos jóvenes que han informado que el envío de contenidos sexuales online constituye una práctica frecuente (Drouin et al., 2013). Los contenidos sexuales fueron con mayor frecuencia enviados a las parejas, seguido del envío a amigos o conocidos offline y, por último, a personas desconocidas o que solo se conocen por Internet, en congruencia con lo informado previamente (e.g., The National Campaign to Prevent Teen and Unplanned Pregnancy, 2008).

Respecto a la VSO, los resultados pusieron de manifiesto que más de un 37% de la muestra reconoció haber sufrido algún tipo de VSO. La mayoría de los casos de VSO fueron de naturaleza leve (i.e., insistir a pesar de la negativa de la víctima), mientras que los tipos más severos como recibir amenazas y difusión de imágenes sexuales sin el consentimiento de la víctima oscilaron entre el 4.6% y el 3.7%, respectivamente. Estos datos expanden la evidencia empírica previa obtenida entre adolescentes y adultos jóvenes (e.g., Goodson et al., 2001; Mitchell et al., 2007) al informar de la prevalencia de un mayor número de tipos de victimización entre adultos de un mayor rango de edades.

Respecto al sexo, como en la mayoría de estudios previos (Benotsch et al., 2012; Reyns et al., 2013; Weisskirch y Delevi, 2011), no se encontraron diferencias entre varo-

nes y mujeres en la prevalencia total del sexting. Sin embargo, un análisis más pormenorizado de los tipos de sexting reveló algunas diferencias interesantes. Así, la prevalencia fue mayor para los varones cuando el contenido sexual era enviado a amigos o conocidos offline o a personas que solo se conocían online. No hubo diferencias entre ambos cuando el sexting se producía en la pareja.

En relación con VSO, más mujeres que hombres informaron sufrir este tipo de victimización. Estos datos son coherentes con la amplia investigación previa que ha encontrado que las mujeres son víctimas con mayor frecuencia de agresión y coerción sexual que los varones. Así, como en otros estudios que exploran las diferencias de sexo en la victimización sexual offline (por ejemplo, Gámez-Guadix et al, 2011;Hines y Saudino, 2003), tanto los hombres como las mujeres sufrieron un comportamiento sexualmente coercitivo, pero las tasas para las mujeres fueron más altas.

Los análisis respecto a la prevalencia del sexting y VSO por edades también revelaron importantes resultados. En primer lugar, un porcentaje elevado (por encima del 63%) de adultos mayores de 35 y menores de 45 años reconocieron implicarse en sexting. Por tanto, estas conductas no parecen exclusivas solo de adolescentes o de adultos jóvenes. Al contrario, los datos sugieren que el sexting es una práctica frecuente también entre adultos de mediana edad. Nuestros datos también indicaron que los adultos a partir de 45 años se implican en menor medida que los adultos más jóvenes en conductas de sexting. El descenso del nivel de deseo sexual con la edad (DeLamater y Sill, 2005) y el menor uso que los más mayores hacen de las nuevas tecnologías (Ine, 2012) podrían explicar estos resultados. No obstante, aunque la prevalencia de sexting parece descender a medida que aumenta la edad, un considerable porcentaje de adultos mayores de 45 años participó en sexting (aproximadamente uno de cada cinco). La VSO, por su parte, de manera similar al sexting, parece ser más frecuente entre adultos jóvenes. La VSO descendió progresivamente desde el 43% para adultos entre 25 y 34 años hasta el 37.3% y el 21.4% para adultos entre 35 y 44 años y para mayores de 45, respectivamente. No obstante, este descenso no debería obscurecer que la VSO es un fenómeno relativamente frecuente también entre adultos mayores.

Tanto el sexting como la VSO mostraron una prevalencia significativamente mayor en personas con una orientación no heterosexual (homosexuales y bisexuales) que entre heterosexuales. Es especialmente llamativo que casi el doble de no-heterosexuales que heterosexuales (63.9% frente al 35.5%) reconocieron haber sufrido VSO. Dado que Internet es un lugar en el que las minorías sexuales pueden contactar para mantener interacciones sexuales con otras personas con menor temor a consecuencias sociales negativas (Brown, Maycock y Burns, 2005), es posible que participen en mayor medida en comportamientos de sexting. Este hallazgo es congruente con la evidencia empírica previa que indica que las minorías sexuales usan Internet más que los heterosexuales para buscar parejas sexuales online (Daneback, Månsson y Ross, 2007), lo cual podría exponerlos en mayor medida a los riesgos relacionados con Internet, tal como la VSO.

Finalmente, tal y como se hipotetizó, los resultados mostraron que la participación en sexting incrementó la probabilidad de sufrir VSO. Además, estos resultados fueron consistentes cuando consideramos cada tipo de VSO por separado (i.e., insistir, amenazas, y difusión de la información). Esto es coherente con estudios previos que han informado de una relación entre sexting y una mayor probabilidad de ser víctima de acoso online no específicamente sexual (Reyns et al., 2013; Ybarra, Mitchell, Finkelhor y Wolak, 2007). Estos resultados sugieren que el sexting podría aumentar la exposición a perpetradores proporcionándoles información o imágenes íntimas. Estos contenidos sexuales podrían ser utilizados por los perpetradores para chantajear a la víctima y para conseguir que esta ceda a sus peticiones, tales como revelarles más información personal, mantener cybersexo o encontrarse offline.

2.5.1. Limitaciones del estudio

Este estudio tiene varias limitaciones que deben tenerse en cuenta. La primera de ellas se refiere a la naturaleza trasversal de los datos, por lo cual se ha de ser cauto a la hora de establecer relaciones causales entre las variables. Futuros estudios longitudinales deberían arrojar luz sobre las relaciones temporales entre el sexting y la VSO. En segundo lugar, aunque nuestra muestra es amplia, no es representativa de la población; por ello, se recomienda cautela en la generalización de los resultados. Nuevos estudios deberían replicar y extender los resultados aquí encontrados en otras muestras de adultos. Finalmente, es importante señalar que, aunque este estudio hizo un esfuerzo por medir el sexting y la VSO de forma más exhaustiva y compresiva que en estudios previos, la medición de estos constructos es un ámbito que requiere futuros desarrollos.

2.5.2. Conclusiones e implicaciones para la investigación y la práctica

En resumen, los hallazgos de este estudio indican que el sexting y la VSO son muy frecuentes y parecen ser una característica común de las interacciones interpersonales online durante la edad adulta. La elevada prevalencia de sexting como método de interacción con los compañeros sexuales sugiere que Internet se está convirtiendo en un importante medio para el desarrollo de las relaciones sexuales en cualquier edad. En cuanto a la VSO, los hallazgos indican que se trata de un problema relativamente frecuente también a cualquier edad. Además, el sexting emergió como un importante factor de riesgo para sufrir VSO. Este estudio extiende la evidencia previa al documentar la existencia de estos fenómenos entre adultos mayores y la relación entre ambos.

Finalmente, estos hallazgos tienen importantes implicaciones para la práctica. En primer lugar, ya que el sexting es altamente prevalente a lo largo del ciclo vital, adultos de todas las edades deberían ser informados sobre sus posibles riesgos y educados para emplear con cautela las posibilidades que brindan las nuevas tecnologías. En segundo

lugar, dado que la VSO no es un problema que ocurre exclusivamente entre jóvenes, es importante ampliar la prevención de este problema también a poblaciones de adultos. En tercer lugar, especial atención se debería prestar a las poblaciones en especial situación de riesgo para sufrir victimización, como parece ser el caso de las mujeres y de las minorías sexuales.

Tabla 1. Prevalencia y diferencias de género en Sexting

	Total	Sexo		
		Varones	Mujeres	χ^2
1. Enviar fotos, imágenes o videos a tu pareja con contenido erótico o sexual sobre ti.	27.8%	29.8%	26.7%	0.92
2. Enviar información escrita o mensajes de texto con contenido erótico o sexual sobre ti a tu pareja.	58.3%	56.7%	59.1%	0.47
3. Enviar fotos, imágenes o vídeos con contenido erótico o sexual sobre ti a un amigo/a o a un conocido/a.	12.0%	21.2%	7.0%	36.81***
4. Enviar información escrita o mensajes de texto con contenido erótico o sexual sobre ti a un amigo/a o conocido/a.	27.0%	34.0%	23.2%	11.37**
5. Enviar fotos, imágenes o vídeos con contenido erótico o sexual sobre ti a alguien que has conocido por Internet pero que en ese momento no conocías en persona.	11.1%	18.9%	6.9%	28.21***
6. Enviar información escrita o mensajes de texto con contenido sexual o erótico sobre ti a alguien que has conocido por Internet y que aún no conocías en persona.	17.2%	24.6%	13.2%	17.48***
Total	66.8%	68.2%	66.1%	0.41

*p < .05; **p < .01; ***p < .001.

Tabla 2. Prevalencia y diferencias de género y edad en la VSO

	Total	Sexo		
		Varones	Mujeres	χ^2
1. Insistir para que envíes fotos o vídeos eróticos o sexuales a pesar de que tú no querías.	28.2%	22.0%	31.5%	8.21**
2. Insistir para que reveles información erótica o sexual sobre ti a pesar de que tú no querías.	24.5%	17.1%	28.5%	12.91***

	Total	Sexo		
		Varones	Mujeres	χ^2
3. Insistir para que lleves a cabo algún comportamiento sexual online que tú no querías hacer (por ejemplo, vía webcam).	22.2%	16.6%	25.2%	7.96**
4. Insistir para mantener relaciones sexuales offline a pesar de que tú no querías.	18.7%	18.2%	19.0%	0.07
5. Amenazar para que envíes fotos, imágenes o vídeos con contenido erótico o sexual tuyo.	1.9%	1.8%	1.9%	0.02
6. Amenazar para que reveles información erótica o sexual sobre ti.	1.8%	1.4%	2.1%	0.44
7. Amenazar para que lleves a cabo algún comportamiento sexual en Internet (por ejemplo, vía webcam).	2.1%	1.1%	2.7%	2.27
8. Amenazar a través de Internet para mantener relaciones sexuales offline.	2.2%	2.1%	2.3%	0.02
9. Difundir o colgar en Internet fotos o vídeos con contenido erótico o sexual tuyo sin tu permiso.	1.1%	1.8%	0.8%	1.72
10. Difundir información de carácter erótico o sexual sobre ti sin tu consentimiento.	3.3%	2.5%	3.8%	0.96
Total	38.3%	31.9%	41.6%	7.43***

*p < .05; **p < .01; ***p < .001.

Tabla 3. Regresión logística analysing the relationship bewteen sexting and VSO

	B	S.E.	Wald	OR (IC 95%)
Sexting	0.77	0.13	36.00***	2.15 (1.68- 2.77)
Edad	-0.02	0.01	5.18*	.99 (.96 – .99)
Sexo	0.80	0.20	15.76***	2.22 (1.50 – 3.31)
Orientación sexual	0.96	0.31	9.28**	2.60 (1.41 - 4.82)
Constante	-2.49	0.54	20.99***	0.083

Note. R^2= .12 (Cox & Snell) .17 (Nagelkerke). Model χ^2 (4) = 79.4, p < .001.

*p < .05; **p < .01; ***p < .001

3. REFERENCIAS

Barak, A. (2005). Sexual harassment on the Internet. *Social Science Computer Review, 23*(1), 77-92.

Baumgartner, S. E., Valkenburg, P. M. y Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology, 31*(6), 439-447.

Benotsch, E. G., Snipes, D. J., Martin, A. M. y Bull, S. S. (2012). Sexting, substance use, and sexual risk behavior in young adults. *Journal of Adolescent Health*.

Bramsen, R. H., Lasgaard, M., Koss, M. P., Shevlin, M., Elklit, A. y Banner, J. (2013). Testing a multiple mediator model of the effect of childhood sexual abuse on adolescent sexual victimization. *American Journal of Orthopsychiatry, 83*(1), 47-54.

Brown, G., Maycock, B. y Burns, S. (2005). Your picture is your bait: use and meaning of cyberspace among gay men. *Journal of Sex Research, 42*(1), 63-73.

Calvete, E., Orue, I., Estevez, A., Villardón, L. y Padilla, P. (2010) Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior, 26,* 1128-1135.

Daneback, K., Månsson, S.-A. y Ross, M. (2007). Using the Internet to find offline sex partners. *CyberPsychology & Behavior, 10*(1), 100-107.

DeLamater, J. D. y Sill, M. (2005). Sexual desire in later life. *Journal of Sex Research, 42*(2), 138-149.

Gámez-Guadix, M., Straus, M. A. y Hershberger, S. L. (2011). Childhood and adolescent victimization and perpetration of sexual coercion by male and female university students. *Deviant Behavior, 32*(8), 712-742.

Goodson, P., McCormick, D. y Evans, A. (2001). Searching for sexually explicit materials on the Internet: An exploratory study of college students' behavior and attitudes. *Archives of sexual behavior, 30*(2), 101-118.

Gordon-Messer, D., Bauermeister, J. A., Grodzinski, A. y Zimmerman, M. (2012). Sexting among young adults. *Journal of Adolescent Health*.

Hines, D. y Saudino, K. J. (2003). Gender differences in psychological, physical, and sexual aggression among college students using the Revised Conflict Tactics Scales. *Violence and Victims, 18*(2), 197-2117.

Ine (2012). Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2012.

Mitchell, K. J., Finkelhor, D., Jones, L. M. y Wolak, J. (2012). Prevalence and characteristics of youth sexting: a national study. *Pediatrics, 129*(1), 13-20.

Mitchell, K. J., Ybarra, M. y Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment, 12,* 314-324.

Mitchell, K. J., Wolak, J. y Finkelhor, D. (2007). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet. *Journal of Adolescent Health, 40*(2), 116-126.

Reyns, B. W., Burek, M. W., Henson, B. y Fisher, B. S. (2013). The unintended consequences of digital technology: exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice, 36*(1), 1-17.

Rice, E., Rhoades, H., Winetrobe, H., Sanchez, M., Montoya, J., Plant, A., et al. (2012). Sexually explicit cell phone messaging associated with sexual risk among adolescents. *Pediatrics, 130*(4), 667-673.

Smith, P. K. (2012). Cyberbullying and cyber aggression. In A. B. N. S.R. Jimerson, M.J. Mayer y M.J. Furlong (Ed.), *Handbook of school violence and school safety: International research and practice (2nd ed.).* (pp. 93 -103). New York: Routledge.

Strassberg, D. S., McKinnon, R. K., Sustaíta, M. A. y Rullo, J. (2013). Sexting by high school students: An exploratory and descriptive study. *Archives of sexual behavior, 42*(1), 15-21.

Straus, M. A., Hamby, S. L., Boney-McCoy, S. y Sugarman, D. B. (1996). The revised conflict tactics scales (CTS2) development and preliminary psychometric data. *Journal of family issues, 17*(3), 283-316.

Wachs, S., Wolf, K. D. y Pan, C.-C. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. *Psicothema, 24*(4), 628-633.

Weisskirch, R. S. y Delevi, R. (2011). «Sexting» and adult romantic attachment. *Computers in Human Behavior, 27*(5), 1697-1701.

Whittle, H., Hamilton-Giachritsis, C., Beech, A. y Collings, G. (2012). A review of young people's vulnerabilities to online grooming. *Aggression and violent behavior*.

Wiederhold, B. K. (2011). Should Adult Sexting Be Considered for the DSM? *Cyberpsychology, Behavior, and Social Networking, 14*(9), 481-481.

Wolak, J., Finkelhor, D., Mitchell, K. J. y Ybarra, M. L. (2010). Online «predators» and their victims. *Psychology of violence, 1*, 13-35.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D. y Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics & Adolescent Medicine, 161*(2), 138.

VIOLENCIA EN EL NOVIAZGO A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS: PREVALENCIA, CONTEXTO Y RELACIÓN CON LA VIOLENCIA OFFLINE[1]

Erika Borrajo
Manuel Gámez-Guadix
Esther Calvete
Universidad de Deusto

RESUMEN: El uso de las nuevas tecnologías como herramientas para acosar y controlar a la pareja ha sido, hasta el momento, escasamente estudiado por la literatura. El objetivo del presente estudio fue conocer la prevalencia de la victimización de la violencia en el noviazgo a través de las nuevas tecnologías (VNNT), así como el contexto en el que se produce, y su relación con la violencia offline. La muestra utilizada constó de 433 estudiantes universitarios de entre 18 y 30 años de edad. Los resultados mostraron que más del 50% de los participantes habían sido víctimas de algún tipo de VNNT en los últimos 6 meses de su relación. La forma más frecuente era el uso de las nuevas tecnologías para controlar a la pareja. Además, quien era víctima de VNNT tendía a serlo de forma recurrente. Los datos muestran, asimismo, que estas conductas aparecían, generalmente, en un contexto de celos. Finalmente, los resultados revelaron una relación significativa entre la VNNT y la violencia psicológica offline. Se discuten las limitaciones y las futuras líneas de investigación.

PALABRAS CLAVE: Violencia en el noviazgo; nuevas tecnologías; agresión; control; celos.

El desarrollo de las nuevas tecnologías, como Internet y el teléfono móvil, ha conllevado múltiples beneficios a nivel social e individual y ha propiciado el desarrollo de nuevos entornos sociales. Además, las herramientas de comunicación instantánea (p.ej., Whatsapp) y las redes sociales, han visto aumentado su uso en los últimos años, convirtiéndose en parte imprescindible de nuestras relaciones sociales. No obstante, las nuevas tecnologías también pueden emplearse como una herramienta de control e intimidación (Dimond, Fiesler y Bruckman, 2011; Jaishankar y Sankary, 2006; King-Ries, 2011). En este contexto, son numerosas las investigaciones que han informado de que las nuevas tecnologías son con frecuencia utilizadas para intimidar, acosar o controlar a otros en contextos interpersonales a través de fenómenos como el cyberbullying (Smith, 2012;

1 Esta investigación ha sido financiada por el proyecto concedido a Manuel Gámez-Guadix por el Ministerio de Economía y Competitividad, Ref. PSI2012-31550.

David-Ferdon y Hertz, 2007; Barlett y Gentile, 2012) o el cyberstalking (Sheridan y Grant, 2007; Pittaro, 2007). Estas formas de violencia parecen haberse extendido de igual forma a las relaciones de pareja.

La violencia en las relaciones de noviazgo (VN) constituye un problema social de gran importancia, tanto por su elevada prevalencia (Bonomi et al., 2012; Marquart, Nannini, Edwards, Satanley y Wayman, 2007; Straus, 2004; Wolitzky-Taylor et al., 2008) como por las consecuencias para sus víctimas, que incluyen, entre otras, sintomatología depresiva, trastornos de ansiedad o TEPT (Eshelman y Levendosky, 2012; Teten, Ball, Valle, Noonan y Rosenbluth, 2009; Banyard y Cross, 2008). Los datos de una reciente revisión muestran una prevalencia de la violencia en el noviazgo del 44% para la violencia física y de hasta el 77% para la violencia psicológica (Leen et al., 2013).

Como se ha mencionado, en los últimos años, la violencia en el noviazgo ha incorporado el uso de nuevas tecnologías (Draucker y Martsolf, 2012; Burke, Wallen,Vail-Smith, y Knox, 2011; Muise, Christofides y Desmarais, 2009; Short y McMurray, 2009; Melander, 2010). La violencia en el noviazgo llevada a cabo a través las nuevas tecnologías (VNNT) incluye amenazas, insultos, conductas de humillación o denigración, comportamiento celoso, aislamiento o comportamientos para controlar a la pareja, características que son comunes con la VN offline (Almendros, Gámez-Guadix, Carrobles, Caballeira y Porrúa, 2009; Buesa y Calvete, 2011; Follingstad, 2007; Follingstad y Edmundson, 2010). Sin embargo, a diferencia de la violencia tradicional, la VNNT conlleva elementos específicos, tales como la difusión de fotos o vídeos a través de Internet con imágenes comprometidas sobre la pareja, el uso de las contraseñas de las redes sociales y el correo electrónico de la víctima para espiarla, o el uso de las nuevas tecnologías con el objetivo de controlar qué hace en cada momento o acosarla.

Algunos estudios sobre violencia en las relaciones de noviazgo comienzan a enfatizar la importancia que las nuevas tecnologías pueden llegar a tener en la dinámica de una relación abusiva como medio para ejercer control, humillar o amenazar a la víctima. Algunos estudios muestran tasas de prevalencia de entre el 26,3% en adolescentes (Zweig, Dank, Yahner y Lachman, 2013), y el 50% en universitarios (Burke et al., 2011).

Igualmente, la evidencia empírica sobre las diferencias de género en la prevalencia y frecuencia de VNNT es escasa, y los resultados disponibles son inconsistentes. Entre los escasos estudios, Zweig et al. (2013) encontraron que no había diferencias entre varones y mujeres en la prevalencia de la victimización no sexual de VNNT; sin embargo, la victimización sexual era más frecuente entre mujeres. Por su parte, Burke et al. (2011) encontraron que las mujeres informaban de una mayor victimización que los hombres en comportamientos online para controlar a la pareja. Estos hallazgos contrastan con el consistente cuerpo de investigación sobre la violencia psicológica offline en los que se ha encontrado que, en términos generales, este tipo de victimi-

zación es más frecuente entre varones (Corral y Calvete, 2006; Harned, 2001; Hines y Saudino, 2003; Muñoz-Rivas, Graña, O´Leary y González, 2007; Straus, Hamby, Boney-McCoy y Sugarman, 1996).

Por otra parte, diferentes trabajos indican la importancia y la necesidad de considerar el contexto en el que se produce para entender mejor la violencia en la pareja en relaciones de noviazgo. Por ejemplo, Muñoz-Rivas, Graña Gómez, O'Leary y González Lozano (2007) encontraron que la mayor parte de las agresiones offline en relaciones de noviazgo ocurrían en un contexto de juego o broma. Otros hallazgos sugieren que los celos y estar enfadado con la pareja podrían constituir también elementos importantes del contexto en el cual la agresión contra la pareja tiene lugar (Fernández-Fuertes y Fuertes, 2010; Sunday, Kline, Labruna, Pelcovitz, Salzinger y Kaplan, 2011). No obstante, la evidencia empírica sobre el contexto en el que tiene lugar la VNNT ha sido, hasta nuestro conocimiento, inexistente.

Otra cuestión adicional de gran relevancia es si la VNNT se produce de manera conjunta con la violencia en la pareja offline como, por ejemplo, la violencia física y psicológica. Se ha argumentado que las nuevas tecnologías podrían constituir un medio de llevar a cabo comportamientos agresivos que el perpetrador no haría cara a cara (Smith, 2012). Asimismo, se ha señalado, incluso, que la VNNT podría disminuir la amenaza de violencia física (Melander, 2010) siendo estas herramientas un posible medio canalizador de esta. Una segunda posibilidad es que la VNNT constituya una modalidad de violencia psicológica en la pareja y, por tanto, la VNNT y la violencia psicológica offline tiendan a coocurrir y estar relacionadas. En esta línea, la VNNT también podría estar relacionada con la violencia física, puesto que la violencia física y la psicológica a menudo aparecen relacionadas (Almendros et al., 2009). Los escasos estudios llevados a cabo hasta el momento parecen apoyar esta segunda hipótesis, al menos entre adolescentes (Cutbush, William, Miller, Gibbs y Clinto-Sherrod, 2012; Hinduja y Patchin, 2011; Zweig et al., 2013). Sin embargo, hasta la fecha, ningún estudio ha analizado la relación entre la VNNT y violencia offline entre adultos en relaciones de noviazgo.

1. EL PRESENTE ESTUDIO

El primer objetivo de este estudio consistió en analizar la prevalencia y la frecuencia, junto con las diferencias de género, de la VNNT entre estudiantes universitarios. El segundo objetivo de este estudio fue examinar el contexto en el cual se produce la VNNT (celos, juego, reciprocidad). Finalmente, el tercer objetivo consistió en analizar la relación de la VNNT con la violencia offline (i.e., violencia física y psicológica). Esto permitirá entender la medida en la cual la VNNT ocurre de forma conjunta con la violencia offline o si, por el contrario, las nuevas tecnologías podrían canalizar comportamientos violentos que no son llevados a cabo cara a cara.

1.1. Método

1.1.1. Participantes

La muestra inicial estuvo compuesta por 529 estudiantes universitarios de ambos sexos. Para el presente estudio, fueron incluidos únicamente aquellos participantes que había tenido o estaban actualmente en una relación de noviazgo (81,85% de la muestra total). Así, la muestra final consistió en 433 estudiantes universitarios (60% mujeres, 37% varones, y 3% no indicaron sexo) con una edad media de 20,39 años (DT=2,06; rango = 18-30 años). El 55% de ellos tenía actualmente pareja y el 45% habían estado en una relación de pareja estable. La duración media de las relaciones fue de 20.30 meses (DT = 18.86).

1.1.2. Medidas

Cuestionario sociodemográfico. Se incluyeron una serie de preguntas sobre la edad, el sexo, si el participante tiene o ha tenido pareja, tipo de relación (heterosexual u homosexual) y la duración de esta en meses.

Violencia en la pareja a través de las nuevas tecnologías. Para el presente estudio, elaboramos nueve preguntas específicas para evaluar la frecuencia con la que los participantes habían sido víctimas de VNNT. Se les pidió a los participantes que nos indicasen el número de veces en que sus parejas o exparejas habían mostrado las siguientes conductas usando las nuevas tecnologías (Internet o el teléfono móvil) en los últimos seis meses de su relación: a) Enviar mensajes amenazantes; b) Enviar mensajes insultantes o humillantes; c) Mandar o colgar fotos o videos para avergonzarte o humillarte; d) Extender rumores, chismes o bromas sobre ti para ridiculizarte; e) Utilizar tus contraseñas para acceder a tus mensajes y/o tus contactos; f) Difundir secretos, información o imágenes comprometidas sobre ti; g) Utilizar las nuevas tecnologías para controlar dónde has estado y con quién; h) Colgar o enviar fotos con otro/a chico/a para ponerte celoso/a and e) Usar las nuevas tecnologías para mantener el contacto con su expareja con la intención de darte celos. Los ítems fueron elaborados a partir de una revisión de la literatura sobre violencia en el noviazgo (e.g., Leen et al, 2013), los estudios sobre victimización online (Hinduja y Patchin, 2008; Tokunaga, 2011) y los estudios cualitativos y cuantitativos sobre violencia en parejas a través de las nuevas tecnologías realizados hasta la fecha (e.g., Lyndon, Bond-Raacke y Cratty, 2011). Cada pregunta debía de ser respondida tres veces, especificando con qué frecuencia esas conductas se daban a través de tres herramientas distintas: redes sociales, mensajería instantánea (Whatsapp, Messenger, SMS) y correo electrónico.

Contexto de la agresión. Si el participante había sido víctima de algún tipo de VNNT, se le pedía que indicase el contexto en el que se había producido esta agresión. En concreto debían marcar una o varias de las siguientes opciones: a) en un contexto de celos; b)

en un contexto de juego o bromas; c) en reciprocidad, porque la víctima lo hizo primero; y d) porque él/ella estaba enfadado y quería molestarme o fastidiarme.

Violencia en la pareja offline. La violencia offline fue medida a través de dos preguntas individuales que medían violencia psicológica («Tu pareja te gritó, insultó, amenazó o destruyó algo que te pertenecía») y violencia física («Tu pareja te empujó, te dio un bofetón o te golpeó»). Se pidió expresamente a los participantes que indicaran la frecuencia con la que estas conductas habían ocurrido *sin* emplear las nuevas tecnologías durante los últimos seis meses de su relación. Ambos ítems fueron respondidos en una escala de cuatro puntos: 0 = *nunca*, 1 = *una o dos veces*, 2 = *tres o cuatro veces*, and 3 = *5 o más veces*.

1.2. Procedimiento

La elección de las aulas en las que se completaron los cuestionarios se llevó a cabo de manera aleatoria entre las diferentes aulas de las distintas facultades. Antes de repartir los cuestionarios, los investigadores informaron del objetivo del estudio y que la participación era voluntaria y anónima. Además, se les facilitó el correo electrónico de uno de los investigadores en caso de querer obtener más información sobre el estudio. La duración aproximada de la aplicación fue de 20 minutos. El proyecto fue revisado y aprobado por el Comité de Ética de la Universidad de Deusto.

2. RESULTADOS

La Tabla 1 presenta la prevalencia y las diferencias de género para cada uno de los tipos de VNNT estudiados. Como puede observarse, aproximadamente la mitad de los jóvenes reconocieron haber sido víctimas de algún tipo de VNNT. No se encontraron diferencias en la victimización entre varones y mujeres (varones: 51.6%; 50.4% mujeres; χ^2 (1 gl, N=433) = 0.05, *ns*). Considerando la prevalencia de los comportamientos de VNNT individuales, los porcentajes oscilaron entre el 1% («tú pareja ha mandado o colgado fotos o vídeos para avergonzarte o humillarte») y el 38.6% («tu pareja ha utilizado las nuevas tecnologías para controlar con quién estabas o qué hacías»). Un considerable porcentaje (17%) también reconoció que su pareja utilizaba sus contraseñas para curiosear sus mensajes y/o sus contactos. En la mayoría de los comportamientos considerados no se encontraron diferencias en la prevalencia entre varones y mujeres. Únicamente, un porcentaje significativamente mayor de hombres que de mujeres informó que su pareja había difundido secretos, información o imágenes comprometidas sobre él sin su consentimiento (varones: 8.3%, mujeres: 3.1%; χ^2 (1 gl, N=433)= 5.36, $p < .05$).

Tabla 1. Prevalencia y diferencias de género de la violencia en la pareja a través de las nuevas tecnologías

	Prevalencia			
	Total	Varones	Mujeres	χ^2
1. Tu pareja te ha enviado mensajes amenazantes	6.5%	8.8%	5.1%	2.27
2. Tu pareja te ha enviado mensajes insultantes o humillantes	7.5%	8.3%	7%	0.21
3. Tu pareja ha mandado o colgado fotos o videos para avergonzarte o humillarte	1%	1.3%	0.8%	0.23
4. Tu pareja ha extendido rumores, chismes o bromas sobre ti para ridiculizarte	3.4%	3.8%	3.1%	0.13
5. Tu pareja utiliza tus contraseñas para curiosear tus mensajes y/o tus contactos.	17%	17.8%	16.5%	0.12
6. Tu pareja ha difundido secretos, información o imágenes comprometidas sobre ti	5.1%	8.3%	3.1%	5.36*
7. Tu pareja ha utilizado las nuevas tecnologías para saber controlar has estado y con quién	38.6%	40.6%	37.4%	0.44
8. Tu pareja ha colgado o enviado fotos con otro/a chico/a para ponerte celoso/a.	14.3%	15.9%	13.2%	0.57
9. Tu pareja ha utilizado las nuevas tecnologías para mantener el contacto con su expareja con la intención de darte celos	15.5%	19.1%	13.3%	2.52

*$p<.05$

También fueron analizadas la frecuencia y la cronicidad de la VNNT. Los resultados se presentan en la Tabla 2. Como puede observarse en la mitad izquierda de la tabla, las conductas con una mayor frecuencia fueron las relacionadas con el control de la pareja y con el uso de las contraseñas para curiosear el correo/redes sociales de la pareja. Con el objetivo de obtener una idea más precisa sobre la frecuencia de cada tipo de agresión solo entre aquellos que la han sufrido, calculamos la cronicidad de la VNNT (Straus y Ramirez, 2007). Los datos de cronicidad se presentan en la mitad derecha de la Tabla 2. Como puede observarse, aquellos participantes que llevaron a cabo alguna conducta de VNNT, tendieron a repetirla en numerosas ocasiones. La cronicidad media de todos los comportamientos de VNNT fue de alrededor de 23 veces en los últimos seis meses. No hubo diferencias de sexo tampoco en cuanto a frecuencia y cronicidad.

Tabla 2. Frecuencia y Cronicidad de la VPNT

	Frecuencia				Cronicidad			
	Total	Varones	Mujeres	t	Total	Varones	Mujeres	t
1. Tu pareja te ha enviado mensajes amenazantes	0.32 (1.57)	0.47 (1.95)	0.25 (1.33)	1.38	5.14 (3.88)	5.36 (4.25)	4.92 (3.59)	0.28
2. Tu pareja te ha enviado mensajes insultantes o humillantes	0.42 (2.25)	0.49 (2.69)	0.36 (1.90)	0.60	5.62 (6.27)	7.65 (2.12)	5.35 (1.26)	0.38
3. Tu pareja ha mandado o colgado fotos o videos para avergonzarte o humillarte	0.02 (0.26)	0.01 (0.17)	0.02 (0.31)	-0.16	2.25 (1.89)	1.50 (0.70)	3 (2.82)	-0.72
4. Tu pareja ha extendido rumores, chismes o bromas sobre ti para ridiculizarte	0.21 (1.61)	0.33 (2.34)	0.15 (0.98)	1.05	6.5 (6.48)	8.66 (9.30)	4.87 (2.99)	1.92
5. Tu pareja utiliza tus contraseñas para curiosear tus mensajes y/o tus contactos.	1.43 (5.46)	1.70 (5.63)	1.30 (5.48)	0.70	8.44 (10.86)	9.57 (10.26)	7.95 (11.50)	0.60
6. Tu pareja ha difundido secretos, información o imágenes comprometidas sobre ti	0.24 (1.78)	0.48 (2.74)	0.10 (0.77)	2.04	4.85 (6.60)	5.76 (8.05)	3.37 (3.06)	0.79
7. Tu pareja ha utilizado las nuevas tecnologías para saber controlar has estado y con quién	9.39 (20.22)	9.54 (22.70)	8.20 (21.90)	0.67	22.14 (30.71)	23.47 (30.78)	21.95 (31.42)	0.30
8. Tu pareja ha colgado o enviado fotos con otro/a chico/a para ponerte celoso/a	0.84 (3.02)	0.83 (2.78)	0.83 (3.17)	-0.003	5.86 (5.91)	5.20 (5.16)	6.26 (6.57)	-0.67
9. Tu pareja ha utilizado las nuevas tecnologías para mantener el contacto con su expareja con la intención de darte celos.	1.34 (5.88)	2.07 (9.65)	0.88 (3.46)	1.82	8.85 (14.68)	10.86 (20.06)	6.64 (7.29)	1.14
Total	2.99 (5.86)	2.13 (4.72)	2.43 (5.14)	1.53	23.33 (26.93)	26.08 (27.72)	21.77 (26.63)	0.51

Respecto a los medios a través de los cuales se experimentó la VNNT, algo más de la mitad del total de los comportamientos (52,04%) fueron llevados a cabo a través de sms o aplicaciones de mensajería (e.g., Whatsapp), el 40,92% a través de redes sociales y un 7,04% a través del correo electrónico.

Asimismo, a aquellos participantes que informaron que habían sido víctimas de al menos un comportamiento de VNNT, les pedimos que especificasen el contexto en el cual se había producido el incidente. El 51.4% informó que su pareja lo hizo en un contexto de celos, el 26.1% porque estaban jugando o bromeando, el 23.9% en reciprocidad (i.e., «ocurrió porque yo se lo hice primero») y el 12.8% indicó que la pareja estaba enfadada y quería fastidiarle o molestarle. No se encontraron diferencias de género en el contexto en el cual se produjo la VNNT.

Finalmente, analizamos si la VNNT estaba relacionada con la violencia offline (física y psicológica). Para ello, en primer lugar, calculamos las correlaciones bivariadas entre la VNNT y la VN psicológica y física offline. Ambas correlaciones fueron estadísticamente significativas (r = .29 para la agresión psicológica y r = .20 para la física; ambas $p < .001$). La relación entre VN psicológica y física offline fue aún más elevada (r = .48, $p < .001$).

En segundo lugar, estimamos un modelo de regresión lineal múltiple incluyendo la violencia en el noviazgo física y psicológica como variables independientes y la VNNT como variable dependiente. Además, incluimos como controles aquellas variables demográficas que mostraron una correlación bivariada significativa con la VNNT: la edad ($r = .16$; $p < .01$), estar actualmente en una relación ($r = .17$, $p < .001$) y la orientación sexual ($r = .13$, $p < .01$), pero no la duración total de la relación ($r = -.09$, $p < .10$) ni el sexo ($r = -.07$, $p = .14$).

Los resultados se presentan en la Tabla 3. Como puede observarse, la violencia física offline no se asoció significativamente con la VNNT, una vez controlado el efecto de la violencia psicológica offline y de las variables control. En cambio, la violencia psicológica sí mostró una relación estadísticamente significativa con la VNNT ($\beta = .19$; $p < .001$).

Tabla 3. Análisis de regresión lineal múltiple sobre la relación de la VPNT y la violencia en el noviazgo offline física y psicológica.

Variables independientes	Variable dependiente: VPNT			
	B	SE	b	t
Violencia offline				
Violencia psicológica	.56	.12	. 25	4.56***
Violencia física	.23	.21	.06	1.10 *ns*

Variables independientes	Variable dependiente: VPNT			
	B	SE	b	t
Variables control				
Edad	-.13	.04	-.16	-3.26**
Pareja actualmente	.45	.17	.13	2.71**
Orientación sexual	-.1.29	..47	-.13	-2.75**

Note. *ns*: non significant; $^{*}p < .05$, $^{**}p < .01$, $^{***}p<.001$.

3. DISCUSIÓN

La finalidad del presente estudio consistió en analizar la extensión y el contexto de la VNNT, y la relación de esta con la VN offline (física y psicológica). Los datos sugieren que la VNNT constituye una forma frecuente de relacionarse entre parejas jóvenes que, además, parece estar relacionada con conductas de violencia psicológica offline. Este estudio amplía la escasa evidencia empírica sobre este novedoso tipo de violencia en el noviazgo de jóvenes adultos.

Los resultados obtenidos mostraron una elevada prevalencia de la VNNT, superior al 50% en los últimos 6 meses de la relación. Las formas más frecuentes de VNNT son las que implican alguna forma de control de la pareja (p.ej., utilizar las nuevas tecnologías para controlar con quién está o qué hace; aproximadamente uno de cada cuatro) y las que implican el uso de las contraseñas de las redes sociales o direcciones de correo electrónico de la pareja para espiarla (aproximadamente uno de cada seis). La prevalencia en este estudio es similar a aquella encontrada en el estudio previo de Burke et al. (2011) quienes también informaron que aproximadamente el 50% de los universitarios se había implicado en VNNT. Sin embargo, aunque los datos no son directamente comparables, debido a la diferencia de edad de las muestras empleadas, la prevalencia hallada en el presente estudio es más elevada a la encontrada previamente en estudios con preadolescentes (Cutbush et al., 2012) y adolescentes (Zweig et al., 2013). En comparación con los adolescentes, el mayor acceso de los adultos jóvenes a dispositivos electrónicos más sofisticados, tales como los Smartphones, podría explicar esta mayor prevalencia ya que estos dispositivos permiten una conexión permanente a Internet y las redes sociales. En cualquier caso, los datos ponen de manifiesto que un elevado porcentaje de los adultos jóvenes han sido víctimas de comportamientos de control e intimidación por parte de las parejas a través de las nuevas tecnologías.

Este estudio amplía la evidencia previa al analizar la frecuencia con que diversos tipos de VNNT eran experimentados entre las víctimas (i.e. cronicidad de las agresiones). Los resultados sugieren que aquellos que fueron víctimas de algún tipo de VNNT,

tendían a serlo de manera recurrente. De esta forma, los participantes que habían sido víctimas de VNNT reconocieron una media de 23 conductas distintas de VNNT en los últimos seis meses. Una posible explicación es que tal vez determinadas conductas de VNNT, tales como el control constante de dónde o con quién está la pareja, sean interpretadas como muestras aceptables de preocupación y amor, tendiendo así a normalizar y a repetir estos comportamientos dentro de la relación de pareja (Redondo, Ramis, Girbis y Schubert, 2011).

En general, no se encontraron diferencias de género significativas en cuanto a la victimización en VNNT se refiere, lo cual apoya lo encontrado por Zweig et al. (2013) entre adolescentes. Estos datos son también congruentes con la mayoría de los estudios previos sobre victimización online no sexual, en los que no se han encontrado diferencias significativas entre varones y mujeres (Tokunaga, 2011). Un único comportamiento consistente en un tipo de agresión relacional (i.e. «Tu pareja ha difundido secretos, información o imágenes comprometidas sobre ti») mostró una mayor prevalencia entre los varones. Tal vez la mayor tendencia de las mujeres a implicarse en agresiones relacionales (e.g., extender rumores) en contraposición con los varones, con más tendencia a las agresiones directas (e.g., agresiones físicas), podría explicar este resultado (Björkqvist, 1994; Card, Stucky, Sawalani y Little, 2008; Owens, Shute y Slee, 2000).

En este estudio, los datos de prevalencia fueron complementados con el análisis del contexto en el cual ocurre la VNNT, lo cual reveló interesantes resultados. En primer lugar, los resultados indican que la mayoría de las agresiones tienden a producirse en un contexto de celos. Así, los celos parecen representar un importante precursor de la VNNT (Muise et al., 2009). En este sentido, algunas conductas de VNNT, tales como intentar controlar a la pareja a través de medios electrónicos o revisar las cuentas de correo o las redes sociales de las parejas, podrían constituir un mecanismo de refuerzo negativo, aliviando el malestar a corto plazo cuando el individuo se siente inseguro y celoso respecto a su pareja. Sin embargo, estos comportamientos, a su vez, es probable que den como resultado interpretaciones erróneas de la información, provocando de esta manera más celos y más episodios de VNNT a medio y largo plazo (Muise et al., 2009). En segundo lugar, más del 25% de los adolescentes indicó que las agresiones se produjeron en un contexto de juego o broma, lo cual es congruente con lo hallado en los estudios previos sobre VN offline (Muñoz-Rivas et al., 2007). Una posible explicación es que los participantes perciben la VNNT como una conducta «sin importancia», que forma parte de la interacción normal de la pareja, y por tanto tiendan a trivializarla como «una broma». Futuros trabajos deberían aclarar si la intensidad y severidad de la agresión llevada a cabo en un contexto de juego o broma es diferente (i.e., más leve) de aquella motivada por los celos o el enfado. En tercer lugar, un considerable porcentaje de los adolescentes (en torno al 23%) indicaron que la agresión fue recíproca, esto es, que sus parejas las habían llevado a cabo porque los participantes se lo hicieron primero. Estos resultados sugieren que un elevado número

de las agresiones son bidireccionales entre ambos miembros de la pareja. Este hallazgo es congruente con la investigación sobre VN offline, en la que se ha encontrado que con frecuencia las agresiones son bidireccionales, y ambos miembros de la pareja pueden ser tanto víctimas como agresores (Archer, 2000; Straus et al., 1996; Swahn, Alemdar y Whitaker, 2010), así como con los estudios sobre cyberbullying que muestran una gran reciprocidad entre perpetración y victimización (Estevez, Villardón, Calvete, Padilla y Orue, 2010; Kowalski y Limber, 2007). En definitiva, estos resultados ponen de manifiesto la necesidad de adoptar una perspectiva situacional para entender el contexto en el cual ocurre la agresión en el noviazgo también en el caso específico de la VNNT.

Los hallazgos indicaron que la VNNT está relacionada con la violencia offline en la pareja, concretamente con la violencia psicológica. Estos datos apoyan los obtenidos por estudios previos entre adolescentes (Zweig et al., 2013; Cutbush et al., 2012), en los que las autoras encontraron que la VNNT tiende a coocurrir con la violencia psicológica offline. Asimismo, estos resultados apoyan la noción de que quienes se implican en la violencia offline también es más probable que se impliquen en VNNT. Por el contrario, la VNNT no parece ser un comportamiento sustitutivo de la violencia offline entre aquellos que no se atreven a llevar a cabo la agresión cara a cara (Melander, 2010). Más aun, la VNNT parece implicar, al igual que la violencia psicológica offline, estrategias de control, insultos y amenazas (Lyndon et al., 2011; Melander, 2010). No obstante, es importante señalar también que el tamaño de la relación entre ambas fue sólo moderado (aproximadamente, de .30), lo cual podría estar indicando que la VNNT presenta elementos y características específicas y diferenciadas de la violencia psicológica tradicional. Futuros estudios deberían analizar los elementos comunes y diferenciales entre la VNNT y la VN offline.

Este estudio presenta varias limitaciones que conviene tener presentes. En primer lugar, los datos estuvieron basados en medidas de autoinforme, lo cual podría haber introducido sesgos en el recuerdo de los participantes sobre incidentes de VNNT. Además, nosotros evaluamos la presencia de cada tipo de VN offline a través de una única pregunta directa, lo cual podría haber limitado la posibilidad de detectar la ocurrencia de algunos de estos comportamientos. Futuros trabajos deberían emplear medidas con unas propiedades psicométricas bien establecidas para medir la presencia violencia en la pareja offline (e.g. CTS2; Straus et al., 1996). En segundo lugar, la muestra seleccionada estuvo compuesta por estudiantes universitarios, por lo que deberíamos de ser cautos a la hora de generalizar los resultados. Futuros estudios deberían replicar estos resultados en otras muestras de adultos. Finalmente, el diseño transversal de este estudio no permite establecer relaciones temporales entre la VNNT y la VN offline. A este respecto, la violencia en la pareja offline podría preceder a la VNNT o viceversa. Igualmente, también es posible que las relaciones entre ellas sean bidireccionales. Futuras investigaciones longitudinales deberían analizar estas cuestiones.

En conclusión, el presente estudio amplía la escasa evidencia empírica sobre la VNNT obtenida hasta el momento. Según nuestros datos, las nuevas tecnologías parecen tener un papel importante en las relaciones de noviazgo y en las disputas que se producen entre ambas partes de la pareja. Este estudio extiende los hallazgos sobre la relación entre VNNT y violencia offline, que se basaban en muestras de adolescentes, replicando esta relación entre estudiantes universitarios. Además, el presente estudio es el primero que, hasta nuestro conocimiento, analiza el contexto en el cual se produce la VNNT. Los resultados tienen diferentes implicaciones para la intervención. En primer lugar, dado que las nuevas tecnologías parecen un medio común para perpetrar agresiones contra la pareja, los programas preventivos de VN deberían trabajar específicamente la VNNT. Asimismo, los programas de prevención deberían incidir en el aprendizaje de estrategias para el manejo de determinadas situaciones (e.g., situaciones de celos) que parecen estar relacionadas con una mayor probabilidad de la VNNT. Asimismo, parece importante actuar sobre las actitudes que apoyan la justificación de estas agresiones en determinados contextos (i.e., «está justificado si la pareja te provoca celos», «la agresión es un broma», «está justificado porque ella/el me lo hizo a mí», etc.). Finalmente, en términos de investigación, futuros estudios deberían analizar los potenciales predictores y consecuencias de la VNNT utilizando un diseño longitudinal, que es uno de los principales retos en la investigación futura en relación con este problema.

4. REFERENCES

Almendros, C., Gámez Guadix, M., Carrobles, J. A., Rodríguez Caballeira, Á. y Porrúa, C. (2009). Abuso psicológico en la pareja: aportaciones recientes, concepto y medición. *Psicología Conductual*, *17*, 433-451.

Archer, J. (2000). Sex differences in physical aggression to partners: A reply to Frieze (2000), O'Leary (2000), and White, Smith, Koss, and Figueredo (2000). *Psychological Bulletin*, *126*(5), 697.

Banyard, V. L., & Cross, C. (2008). Consequences of teen dating violence understanding intervening variables in ecological context. *Violence Against Women*, *14*, 998-1013.

Barlett, C. P., & Gentile, D. A. (2012). Attacking Others Online. *Psychology of Popular Media Culture*, *1*, 123-135.

Björkqvist, K. (1994). Sex differences in physical, verbal, and indirect aggression: A review of recent research. *Sex Roles*, *30*, 177-188.

Bonomi, A. E., Anderson, M. L., Nemeth, J., Bartle-Haring, S., Buettner, C., & Schipper, D. (2012). Daring violence victimization across the teen years: Abuse frequency, number of abusive partners, and age at first occurrence. *BMC Public Health, 12*, 637-646.

Buesa, S. y Calvete, E. (2011). Adaptación de la escala de abuso psicológico sutil y manifiesto a las mujeres en muestra clínica y de la comunidad. *Anales de Psicología*, *27*, 774-782.

Burke, S. C., Wallen, M., Vail-Smith, K., & Knox, D. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. *Computers in Human Behavior*, *27*, 1162-1167.

Card, N. A., Stucky, B. D., Sawalani, G. M., & Little, T. D. (2008). Direct and indirect aggression during childhood and adolescence: A meta-analytic review of gender differences, intercorrelations,and relations to maladjustment. *Child Development, 79,* 1185-1229.

Corral, S., & Calvete, E. (2006). Evaluación de la violencia en las relaciones de pareja mediante las Escalas de Tácticas para Conflictos: Estructura factorial y diferencias de género en jóvenes. *Psicología Conductual,2,*, 215-234.

Cutbush, S., Williams, J., Miller, S., Gibbs, D., & Clinton-Sherrod, M. (2012). Electronic dating aggression among middle school students: demographic correlates and associations with other types of violence. In *Poster presented at the American Public Health Association, annual meeting, October* (pp. 27-31).

David-Ferdon, C., & Hertz, M. F. (2007). Electronic media, violence, and adolescents: An emerging public health problem. *Journal of Adolescent Health*, *41*, S1-S5.

Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with Computers*, *23*, 413-421.

Draucker, C. B., & Martsolf, D. S. (2010). The role of electronic communication technology in adolescent dating violence. *Journal of Child and Adolescent Psychiatric Nursing, 23*, 133-142.

Eshelman, L., & Levendosky, A. A. (2012). Dating violence: mental health consequences based on type of abuse. *Violence and Victims*, *27*, 215-228.

Estévez, A., Villardón, L., Calvete, E., Padilla, P., & Orue, I. (2010). Adolescentes víctimas de cyberbullyng: prevalencia y características. *Psicología Conductual*, *18*, 73-89.

Fernández-Fuertes, A. A., & Fuertes, A. (2010). Physical and psychological aggression in dating relationships of Spanish adolescents: Motives and consequences. *Child Abuse & Neglect*, *34*, 183-191.

Fritz P. (2006). Attributions for partner aggression in specific incidents of aggression. Dissertation Abstracts International: Section B: The Sciences and Engineering; 66(9-B):5086.

Follingstad, D. R. (2007). Rethinking current approaches to psychological abuse: Conceptual and methodological issues. *Aggression and Violent Behavior*,*12*, 439-458.

Follingstad, D., & Edmundson, M. (2010). Is psychology abusereciprocal in intimate relationships? Data from a National sample of American adults. *Journal Of Violence, 25,* 495-508.

Harned, M. S. (2001). Abused women or abused men? An examination of the context and outcomes of dating violence. *Violence and Victims*, *16*, 269-285.

Hines, D. A., & Saudino, K. J. (2003). Gender differences in psychological, physical, and sexual aggression among college students using the Revised Conflict Tactics Scales. *Violence and Victims*, *18*(2), 197-217.

Hinduja, S. & Patchin, J. W. (2011). Electronic dating violence: A brief for educators and parents. Cyberbullying Research Center (www.cyberbullying.us).

Jaishankar, K., & Sankary, V. U. (2006). *Cyber Stalking: A global menace in the information super highway.* Paper presented at the 29th All Indian Criminology Conference, Madurai Kamaraj University, Madurai, India. Paper retrieved from: http://www.selfhelpmagazine.com/maheu/all-about-cyber-stalking/

King Ries, A. (2011). Teens, technology, and cyberstalking: The domestic violence wave of the future? *Texas Journal of Women and the Law, 20*, 131-193.

Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health*, *41*, S22-S30.

Leen, E., Sorbring, E., Mawer, M., Holdsworth, E., Helsing, B. & Bowen, E. (2013). Prevalence, dynamic risk factors and the efficacy of primary interventions for adolescent dating violence: An international review. *Aggression and Violent Behavior*, *18*, 159-174.

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking*, *14*, 711-716.

Marquart, B. S., Nannini, D. K., Edwards, R. W., Satanley, L. R, & Wayman, J. C. (2007). Prevalence of dating violence victimization: Regional and gender differences. *Adolescence, 42*, 645-657.

Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking*, *13*, 263-268.

Muise, A., Christofides, E., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?. *CyberPsychology & Behavior*, *12*(3), 341-345.

Muñoz-Rivas, M. J., Graña Gómez, J. L., O'Leary, K. D. y González Lozano, P. (2007). Aggression in adolescent dating relationships: prevalence, justificatin, and health consequences. *Journal of Adolescent Health, 40*, 298-304.

Owens, L., Shute, R., & Slee, P. (2000). «Guess what I just heard!»: Indirect aggression among teenage girls in Australia. *Aggressive behavior*, *26*, 67-83.

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, *1*, 180-197.

Redondo, G., Ramis, M., Girbis, S. y Schubert, T. (2011). Attitudes on Gender Stereotypes and Gender-based Violence among Youth. Daphne III Programme: Youth4Youth: Empowering Young People in Preventing Gender-based Violence through Peer Education. Retrieved from: http://www.medinstgenderstudies.org/wp-content/uploads/report_dapnhe-Spain_CREA.pdf

Sunday, S., Kline, M., Labruna, V., Pelcovitz, D., Salzinger, S., & Kaplan, S. (2011). The Role of Adolescent Physical Abuse in Adult Intimate Partner Violence. *Journal Of Interpersonal Violence, 26*, 3773-3789.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different?. *Psychology, Crime & Law*, *13*, 627-640.

Short, E., & McMurray, I. (2009). Mobile phone harassment: An exploration of students' perceptions of intrusive texting behavior. Human Technology: An Interdisciplinary Journal On Humans In ICT Environments, 5, 163-180.

Smith, P. K. (2012). Cyberbullying and cyber aggression. In A. B. N. S.R. Jimerson, M.J. Mayer, & M.J. Furlong (Ed.), *Handbook of school violence and school safety: International research and practice (2nd ed.).* (pp. 93 -103). New York: Routledge.

Straus, M. A., Hamby, S. L., Boney-McCoy, S., & Sugarman, D. B. (1996). The revised conflict tactics scales (CTS2) development and preliminary psychometric data. *Journal of Family Issues*, *17*(3), 283-316.

Straus, M. A. (2004). Prevalence of Violence Against Partners by Male and Female Uniersity Students Worldwide. *Violence Against Women, 10*, 790-811.

Straus, M. A., & Ramirez, I. L. (2007). Gender symmetry in prevalence, severity, and chronicity of physical aggression against dating partners by university students in Mexico and USA. *Aggressive Behavior*, *33*, 281-290.

Swahn, M.H., Alemdar, M., & Whitaker, D.J. (2010). Nonreciprocal and Reciprocal Dating Violence and Injury Occurrence among Urban Youth. *Western Journal of Emergency Medicine, 11*, 264-268.

Teten, A. L., Ball, B., Valle, L. A., Noonan, R., & Rosenbluth, B. (2009). Considerations for the definition, measurement, consequences, and prevention of dating violence victimization among adolescent girls. *Journal of Women's Health*, *18*, 923-927.

Tokunaga, R. S. (2011). Social networking site or social surveillance site? understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior, 27*, 705-713.

Wolitzky-Taylor, K. B., Ruggiero, K.J., DAnielson, C., Resnick, H. S., Hanson, R. F., Smith, D. W. & Kilpatrick, D. G. (2008). Prevalence and corretaltes of da-

ting violence in a national sample of adolescents. *Journal of The American Academy Of Child & Adolescent Psychiatry, 47,* 755-762.

Zweig, J. M., Dank, M., Yahner, J., & Lachman, P. (2013). The rate of cyber dating abuse among teens and how it relates to other forms of teen dating violence. *Journal of Youth and Adolescence*, 1-15.

CIVILIAN DIRECT PARTICIPATION IN CYBER HOSTILITIES

François Delerue
Ph.D. researcher in International Law
at the European University Institute

ABSTRACT: This article studies the application of a well-known notion of international humanitarian law, civilian direct participation in hostilities, to cyber warfare.

According to the principle of distinction, civilians and combatants must be distinguished in times of armed conflict. The shift of hostilities from the real world into cyberspace affects neither the definition of combatants nor the negative definition of civilians. However, beyond the classical approach of the principle of distinction, the changing character of warfare also concerns cyber warfare. Indeed, the distinction between battlefields and civilian areas is increasingly less clear and a rising number of non-combatants directly participate in hostilities in various ways. Cyber means, and the development of cyber warfare, offer numerous new possibilities for non-combatants who want to take part in hostilities. It has never been that easy to get involved in hostilities for civilians and most civilians are ignorant of the consequences of their actions.

Recently, two groups of experts have released documents partly related to this topic with divergent conclusions: the first one is the *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* adopted by the ICRC in 2009. The second one is *Tallinn Manual on the International Law Applicable to Cyber Warfare* written at NATO's Cooperative Cyber Defence Centre of Excellence behest. As these documents differ in their approach to reading of the topic, part of this article will analyze their divergences.

KEYWORDS: Cyber Warfare; International Law; Civilians; Armed Conflict; Internet.

1. INTRODUCTION

According to the principle of distinction, civilians and combatants shall be distinguished in times of armed conflict. However, the differentiation between battlefields and civilian areas is less and less clear, and an increasing number of civilians are taking direct part in hostilities in various ways. Cyber means, and the development of cyber warfare, offer numerous new possibilities for civilians who want to take part in hostilities.

First of all, cyber warfare clearly differs from conventional warfare simply because everybody can gain easy access to cyber weapons. Most people today have, indeed, access to a computer and Internet is full of websites, blogs, and forums, which describe how to design a cyber attack, and it is also easy to download ready-to-use computer codes for cyber attacks.

A good illustration of civilians taking direct part in hostilities can be found in the partisans characterized by Carl Schmitt in his famous book titled *Theory of the Partisan*.[1] Schmitt describes four traits that characterize a partisan: irregularity, intense political engagement, tactical versatility and speed, and a 'telluric' character. Irregularity remains an important trait for a cyber partisan, as well as tactical versatility and speed, which is even truer and more relevant in the Internet age. Indeed, through the Internet a cyber partisan can act from wherever he wants, affecting a computer anywhere in the world. But, to me, it seems that the main challenge for Schmitt's theory in the information age concerns the intense political engagement. If a cyber partisan is fighting as a partisan in the real world, he might be aware of the risks; he can, indeed, be injured or even killed during the hostilities. Furthermore, it is not always easy and safe to acquire weapons for the classical partisan; as a consequence, his motives must be strong. But in the information age, it is very easy to be informed about what happens everywhere in the world and to find a way to act: access to *cyber weapons* is very easy. Also, *cyber partisans* are not physically engaged in the hostilities and due to the relative distance between them and the battlefield they can feel that they are immune from the consequences of their actions. This is perhaps one of the biggest shifts of civilian direct participation in cyber warfare. Indeed, it has never been so easy to get involved and most people tend to ignore the consequences of their actions.

Secondly, new technologies are omnipresent in modern battlefields. Consequently, States and their armies, as well as private actors, need the best technicians to use those technologies. It is the same in the case of cyber warfare, and this situation can lead to a large number of civilians involved in cyber hostilities. Sean Watts described this situation perfectly:

> Reports indicate that few information operations experts currently serve as active duty soldiers. Many private companies have employed the skills of those with expertise in the various weapons commonly used in CNA. For example, Panasonic hired a formally convicted computer hacker to monitor its cybersecurity. The government has also hired cybercriminals as «cyberwarriors» or for defensive purposes. Additionally, many of the individuals who conduct CNA attacks have been recruited from various disciplines with- in the military, including intelligence, operations, and communications.[2]

In order to review those different issues, this article addresses the question of civilian direct participation in cyber hostilities, firstly, by defining the notion; secondly, by focusing and comparing the divergent approaches of the *Interpretive Guidance on the*

---

1 Carl Schmitt, *Theory of the Partisan: Intermediate Commentary on the Concept of the Political* (first published 1963, translated by G L Ulmen, Telos Press Publishing 2007).

2 Sean Watts, 'Combatant Status and Computer Network Attacks' (2010) 50 Virginia Journal of International Law 391, 402–403; see also Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge Studies in International and Comparative Law, Cambridge University Press 2012) 160.

Notion of Direct Participation in Hostilities under International Humanitarian Law (hereafter the *Interpretive Guidance*) adopted by the ICRC in 2009 and the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (hereafter the *Tallinn Manual*) written at NATO's Cooperative Cyber Defence Centre of Excellence behest. Moreover, the article addresses two issues more specific to cyber warfare: civilians acting from outside the geographical limits of the armed conflict or who are unaware of their participation.

2. THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES

Nowadays, «civilians saturate the modern battlefield, often engaging in activities that have traditionally been performed by members of the armed forces (combatants)».[3] Under international humanitarian law (IHL) this participation is characterized by the notion of civilian direct participation in hostilities. This notion is not clearly defined in IHL (2.2.) and its foundation can be found in various instruments (2.1.)

2.1. Sources and Legal Value of the Notion of Direct Participation in Hostilities

The notion of civilian direct participation in hostilities is deduced from treaty law applicable to international and non-international armed conflicts. Article 51(3) of Protocol Additional I,[4] which deals with international armed conflicts, and article 13(3) of Protocol Additional II,[5] which deals with non-international armed conflicts, prescribe that civilians shall enjoy general protection against dangers arising from military operations «unless and for such time as they take a direct part in hostilities». The two additional protocols offer the best expression of this limitation of civilian immunity; however, the common article 3 to the Geneva Conventions limits the protection granted to civilians to «persons taking no active part in the hostilities» and that can be seen as an embryonic version of the concept of civilian direct participation in hostilities. The concept of civilian direct participation in hostilities also appears in other instruments, e.g. in the Rome Statute of the International Criminal Court.

This concept is based on the two additional protocols of the Geneva Conventions of 1949. Conversely to the Geneva Conventions, these additional protocols are not

3 Michael N Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 New York University Journal of International Law and Politics 697, 699.

4 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (hereafter Protocol Additional I).

5 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977 (hereafter Protocol Additional II).

universally ratified and they are not entirely recognized as customary international law. For State parties, these two articles are thus binding treaty law, but not for the others.

Several States are not party to these two additional protocols, including important military powers that are currently involved in war situations, notably the United States and Israel. However, the provisions of article 51(3) of Protocol Additional I, and of article 13(3) of Protocol Additional II are considered as part of customary international law.[6] Even States that are not party to the additional protocols recognize this customary value. For example, the Supreme Court of Israel has recognized that «all of the parts of article 51(3) of The First Protocol express customary international law.»[7] In addition, it should be highlighted that «numerous military manuals state that civilians are not protected against attack when they take a direct part in hostilities»,[8] and recognize the notion of civilians taking direct part in hostilities and its consequences.[9]

In sum, as article 51(3) of Protocol Additional I and article 13(3) of Protocol Additional II reflect customary international law, the notion of civilian direct participation in hostilities has the same legal value and content for all States in the world.

2.2. Lack of Definition

Although it is agreed that the notion of civilian direct participation in hostilities is customary international law, most authors also agree that there is a lack of definition of this notion.

Courts and tribunals can work without definition. As the International Criminal Tribunal for the former Yugoslavia (ICTY) pointed out, courts and tribunals try cases a posteriori, which allows for an assessment of situations on a case-by-case basis.[10] Also, the work of the International Committee of the Red Cross (ICRC) on this notion

6 Louise Doswald-Beck and Jean-Marie Henckaerts, *Customary International Humanitarian Law: Volume 1, Rules.* (2004) rule 6, 19–24. See also ICTY, Trial Chamber II, *Prosecutor v. Pavle Strugar* (Judgment), IT-01-42-T, 31 January 2005, 101, § 220.

7 Israel, Supreme Court, Public Committee against Torture in Israel and Palestinian Society for the Protection of Human Rights and the Environment v Israel and others, Judgment, Case HCJ 769/02, 14 December 2006, reproduced in Oxford Report on International Law and Domestic Courts 597 (IL 2006) [hereafter Targeted Killing Case], § 30.

8 Doswald-Beck and Henckaerts (n 6) 20; Michael N Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 Harvard National Security Journal 5, 13.

9 Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) rule 35.

10 ICTY, Trial Chamber, *the Prosecutor v Dusko Tadic a/k/a 'Dule'* (Opinion and Judgment), IT-94-1-T, 7 may 1997, § 616.

started with a case-by-case approach.[11] However, this lack of definition can become problematic during an armed conflict, as Nils Melzer highlighted, since «it leaves military commanders operating in situations of armed conflict without satisfactory guidance as to the legal standards governing the force used in response to civilian violence».[12] Consequently, the practitioners of IHL need a definition or clarification of this notion. This situation explains why the ICRC decided to set up a reflection on this notion.

3. THE ICRC'S *INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW* APPLIED TO CYBER WARFARE

Civilians have become increasingly present and active in battlefields, in two roles in particular: firstly as mercenaries or members of private military companies, and secondly as civilians taking up arms against a perceived enemy. Additionally, it was in reaction to this increased civilian participation that the ICRC decided to set up a project on the notion of civilian direct participation in hostilities, resulting in the publication of the ICRC's *Interpretive Guidance* in 2009.[13]

The ICRC and the TMC Asser conducted this project from 2003 to 2008. Around 50 experts, participating in their private capacity and coming from different backgrounds (academic, military, governmental, and non-governmental), took part in five informal meetings. The project and the *Interpretative Guidance* did «not endeavor to change binding rules of customary or treaty IHL, but reflect[ed] the ICRC's institutional position as to how existing IHL should be interpreted in light of the circumstances prevailing in contemporary armed conflicts.»[14] The project was designed in order to

11 Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 704.

12 Nils Melzer, 'Civilian Participation in Armed Conflict' [2010] Max Planck Encyclopedia of Public International Law § 5.

13 Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross, 2009).

14 Ibid 9; *contra* see Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretive Guidance' (2009) 42 New York University Journal of International Law and Politics 641, 693 ('The Interpretative Guidance is certainly not a re-statement of existing law.'); see also: W Hays Parks, 'Part IX of the ICRC Direct Participation in Hostilities Study: No Mandate, No Expertise, and Legally Incorrect' (2009) 42 New York University Journal of International Law and Politics 769, 794–795; see also the reply formulated in Nils Melzer, 'Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2009) 42 New York University Journal of International Law and Politics 831, 893–894.

address three questions: firstly, «[w]ho is considered a civilian for the purposes of the principle of distinction?»; secondly, «[w]hat conduct amounts to direct participation in hostilities?»; and thirdly, «[w]hat modalities govern the loss of protection against direct attack?».[15]

The notion of civilian direct participation remains however highly controversial, and the final version of ICRC's *Interpretative Guidance* is far from non-contentious; it seems that it was impossible to reach the planned output to produce a consensus document.[16] Some participants pushed for a more restrictive understanding of this notion, which would lead to a more protective status for civilians, and others «consistently advocated for a more permissive targeting regime than is proposed in the Interpretative Guidance».[17] Also, as specified in the *Interpretative Guidance*, it is «an expression solely of the ICRC's views».[18] As the *Interpretative guidance* is highly controversial, the ICRC «took the unusual step of publishing the *Interpretative Guidance* without identifying the participants».[19] Finally, it is important to note that this is a non-binding document for States[20] even if it could influence States' practice.

Nils Melzer, the editor of the *Interpretative Guidance*, has replied to some of the criticisms that have been directed against it.[21] Notably, he listed some issues remaining controversial in his eyes:

> (1) the criteria for distinguishing civilians from members of organized armed groups; (2) the so-called «revolving door» of protection according to which civilians can repeatedly lose and

15 *Interpretive Guidance* (n 13) 13.

16 Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 6.

17 Melzer, 'Keeping the Balance Between Military Necessity and Humanity' (n 14) 834; in this way Michael N. Schmitt, among others, considers that 'the Interpretive Guidance repeatedly takes positions that cannot possibly be characterized as an appropriate balance of the military needs of states with humanitarian concerns. […] Counter-intuitively, non-state actors, who enjoy no combatant privilege, benefit from greater protection than do their opponents in the regular armed forces. It is similarly disturbing that individuals who directly participate on a recurring basis enjoy greater protection than lawful combatants. […] Unfortunately, the Interpretive Guidance, the product of tireless efforts on the part of the ICRC and the experts involved, sets forth a normative paradigm that states that actually go to war cannot countenance.' Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 44; see also Watkin (n 14) 693–694.

18 *Interpretive Guidance* (n 13) 6.

19 Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 6; see also Parks (n 14) 784.

20 *Interpretive Guidance* (n 13) 6.

21 Melzer, 'Keeping the Balance Between Military Necessity and Humanity' (n 14) 831–916.

> regain protection against direct attack; and (3) the restraints imposed on the use of force against legitimate military targets. Finally, although the three defining elements of «direct participation in hostilities,» the core piece of the Guidance, were far less controversial, their application to certain activities, such as voluntary human shielding and hostage taking, still gave rise to significant disagreement among the participating experts.[22]

As noted even by those who criticize the *Interpretative Guidance*, «[t]he work effectively identifies and frames the issues and offers a sophisticated departure point for further mature analysis».[23] One of the critics, Michael N. Schmitt, for instance, highlighted that «the constitutive elements of direct participation, although not bereft of flaws, represent a useful step forward in understanding the notion.»[24]

That being said, this article on direct participation in hostilities and cyber warfare is built upon the *Interpretative Guidance*, as it is the most thorough work on this topic to date. It is important to note that the editor of the *Interpretative Guidance* has published several articles on cyber warfare and, moreover, the *Interpretative Guidance* itself made some references to cyber warfare. These references have been analyzed in a critical perspective by Georg Kerschischnig,[25] for whom «the examples mentioned in the ICRC Guide are not convincing.»[26] In addition, the dispositions on civilian direct participation of *Tallinn Manual* are compared in this article to those of the *Interpretative Guidance.*

This article partly follows the outlines of the *Interpretative Guidance* but it will address only the points that are relevant for its topic: the ICRC's constitutive elements of the notion of direct participation in hostilities (3.1.), its temporal scope (3.2.), and the modalities governing the loss of protection (3.3. and 3.4.).

3.1. The Constitutive Elements of the notion of direct participation in hostilities

The fifth recommendation, on the *constitutive elements of direct participation in hostilities*, is the heart of the *Interpretative Guidance*.[27] Three cumulative criteria have been

22 Ibid 834.

23 Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 44.

24 Ibid 43; see also Bill Boothby, 'And for Such Time as: The Time Dimension to Direct Participation in Hostilities' (2009) 42 New York University Journal of International Law and Politics 741, 768; it should be noted that most of articles and books studying the notion of direct participation in hostilities and cyber warfare refer to the Interpretative Guidance, see e.g. *The Tallinn Manual* (n 9) rule 35.

25 Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing 2012) 207–213.

26 Ibid 209.

27 Melzer, 'Keeping the Balance Between Military Necessity and Humanity' (n 14) 856.

formulated: the threshold of harm (3.1.1.), the direct causation (3.1.2.), and the belligerent nexus (3.1.3.).[28] It must be noted that even though «various experts entertained specific concerns about particular facets of the constitutive elements, most viewed them as, in a very general sense, reflecting the group's broad understanding.»[29]

3.1.1. Threshold of harm

The first cumulative criterion is called the *threshold of harm* and it requires that the «act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack».[30] On one hand, the effects of the act «must be likely to» produce the required consequence but must not necessary have produced it. Thus, the *threshold of harm* can be reached without or before the materialization of the harm; the probability of the harm is sufficient.[31] In this way, «wherever a civilian had a subjective 'intent' to cause harm that was objectively identifiable, there would also be an objective 'likelihood' that he or she would cause such harm.»[32] On the other hand, the *threshold of harm* can be reached alternatively by causing «harm of a specifically military nature or by inflicting death, injury, or destruction on persons or objects protected against direct attack.»[33], It should therefore be highlighted that the threshold is higher when the target is not military.

The *Interpretative Guidance* states that «the interruption of electricity, water, or food supplies, […] the manipulation of computer networks, […] would not, in the absence of adverse military effects, cause the kind and degree of harm required to qualify as direct participation in hostilities.»[34] This is particularly interesting and relevant in the context of cyber warfare. Indeed, cyber attacks can lead to death, injuries or destruction but usually this is an indirect consequence. Therefore, the civilian side of the *threshold of harm*, that is to say causing «death, injuries or destruction on persons or objects protected against direct attack», seems to be difficult, or even impossible, to fulfill by a cyber operation.

---

28 *Interpretive Guidance* (n 13) 16, 46–64; see also Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) passim.

29 Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 27.

30 *Interpretive Guidance* (n 13) 16, 46–50.

31 Ibid 47; Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 724–725.

32 Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 725.

33 *Interpretive Guidance* (n 13) 47.

34 Ibid 50.

The *Interpretative Guidance* focuses on harm that occurs in the real world.[35] If death and injuries are impossible in cyberspace, there can still be damage and destruction of data. Destruction or damage of data could, I think, be seen as reaching the requirement of the *threshold of harm* but we should be very careful on this point. If we include it, we should add a threshold of intensity to it. Indeed, the destruction of patient's data in a hospital database would, from my point of view, reach the *threshold of harm,* whereas the participation in cyber operations against the website of a private company would not.

The military side of the *threshold of harm*, that it must «adversely affect the military operations or military capacity», seems easier to reach by cyber operations. However, we should have in mind that this military side can be too permissive against civilians participating in hostilities without being aware of what could be the consequences of their acts. Cyberspace offers an easy way to express protest against military operations, and perpetrators might not be aware of the legal repercussions of their actions. Also, it seems that most cyber operations might be likely to harm the military but with a very low consequence and the qualification of direct participation can be seen disproportionate in this context.

3.1.2. Direct Causation

The second cumulative criterion is called the *direct causation* and it requires that «there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part».[36] The content of this criterion remains controversial.[37] I will not address the debate on this criterion here but solely analyze it in the perspective of cyber warfare.

Generally, to satisfy the criterion of *direct causation*, a specific act must directly cause or be expected to cause, the harm that satisfies the first criterion (*threshold of harm*) by itself or as an integral part of a collective operation.

Cyber operations do not particularly challenge this criterion. Indeed, even if the act can be perpetrated far from the battlefield that does not affect the causal link between the act and the caused or expected harm.[38]

However, some situations are specific to cyber warfare, for example a civilian who produces a cyber weapon. At first, it seems that this can be compared to the example of assembling and storing of an improvised explosive device (IED) given by the *Inter-*

35 Jody Mailand Prescott, 'Direct Participation in Cyber Hostilities: Terms of Reference for like-Minded States?', *2012 4th International Conference on Cyber Conflict (CYCON)* (2012) 253.

36 *Interpretive Guidance* (n 13) 16, 46, 51–58.

37 See notably Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 725–735.

38 *Interpretive Guidance* (n 13) 55.

pretative Guidance.[39] Even if the assembling and storing of the IED «may be connected with the resulting harm through an uninterrupted causal chain of events, but, unlike the planting and detonation of that device, [it] do[es] not cause that harm directly.»[40] But, in the case of cyber warfare, cyber weapons must be, in most cases, designed for a specific cyber operation. As a consequence, it seems that there is direct causal link between the production of the cyber weapon and the expected harm, and so the producer of it can be qualified as taking direct part in hostilities. In cases of a collective cyber operation, even if a civilian's contribution does not satisfy the causal link on its own, the civilian can be considered as taking direct part in hostilities due to his involvement in the collective operation. The *Interpretative Guidance* illustrates this with the example of people involved in an attack carried out by unmanned aerial vehicles.[41]

3.1.3. Belligerent Nexus

The third and last cumulative criterion, the *belligerent nexus* is «the less controversial of the three».[42] The *belligerent nexus* requires that the «act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another».[43] Also, this criterion is not specifically transformed or affected by cyber warfare and does not require further discussion on it.

However, it should be noted that the *belligerent nexus* requires that direct participation be distinguished from individual self-defense[44] and also from opportunistic criminal activities. In cyberspace this criterion should be analyzed with great care; indeed, direct participation in hostilities and criminal activities can be closely linked and difficult to tell apart.[45]

3.2. Temporal scope of the direct participation in hostilities

The temporal scope can be divided into two questions: what is encompassed in direct participation in hostilities (3.2.1.) and what is its duration (3.2.2.).

---

39 Ibid 54; *contra* Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 31; see also Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 731–732.

40 *Interpretive Guidance* (n 13) 54.

41 Ibid.

42 Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 735.

43 *Interpretive Guidance* (n 13) 16, 46, 58–64; see also Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 735–736.

44 Melzer, 'Civilian Participation in Armed Conflict' (n 12) § 10.

45 Prescott (n 35) 254.

3.2.1. Preparatory measures, deployment and return

According to section VI of the *Interpretative Guidance* titled *Beginning and end of direct participation in hostilities*, «[m]easures preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution, constitute an integral part of that act.»[46]

Preparatory measures must be distinguished whether they aim «*to carry out a specific hostile act* or aim *to establish the general capacity to carry out unspecified hostile acts*»; only the former constitutes an act of direct participation.[47] As noted before, in most cases it seems that the creation of cyber weapons will constitute an act of direct participation, as each cyber weapon needs to be adapted to its target. It is important to note that the temporal or geographical distance from the target of the civilian who directly participates does not affect the qualification of direct participation in hostilities.[48] It should be noted that a few authors criticize this approach and plead for an extension of the qualification of the direct participation in hostilities to acts aiming to increase the general capacity of a belligerent and not only to those linked to a specific act.[49]

On the question of the *deployment and return*, the *Interpretative Guidance* specifically mentions the question of cyber warfare:

> Where the execution of a hostile act does not require geographic displacement, as may be the case with computer network attacks or remote-controlled weapons systems, the duration of direct participation in hostilities will be restricted to the immediate execution of the act and preparatory measures forming an integral part of that act.[50]

It seems that the duration of cyber direct participation is restricted, therefore, to the execution of the act. The trip to the place from where a civilian will launch a cyber attack, and the return from it, cannot be qualified as deployment and return and are not part of the direct participation in hostilities, conversely to the launch of the cyber attack. Nevertheless, the *Tallinn Manual* takes the opposite position:

> Any act of direct participation in hostilities by a civilian renders that person targetable for such time as he or she is engaged in the qualifying act of direct participation. All of the Experts agreed that this would at least include actions immediately preceding or subsequent to the qualifying act. For instance, traveling to and from the location where a computer used to mount an operation is based would be encompassed in the notion.[51]

---

46 *Interpretive Guidance* (n 13) 65.

47 Ibid 66.

48 Ibid.

49 Watkin (n 14) 660–662; Boothby (n 24) 750–751.

50 *Interpretive Guidance* (n 13) 68.

51 *The Tallinn Manual* (n 9) rule 35, § 7.

This distinction seems justified in cases of sporadic acts amounting to direct participation in hostilities. This leads us to the question of the duration of the participation.

3.2.2. Duration

The duration is one of the most controversial parts of the *Interpretative Guidance*.[52] According to the two additional protocols to the Geneva Conventions, a civilian loses his civilian protection «for such time» as he takes direct part in hostilities. Although this phrasing is highly controversial, it is considered customary international law.[53]

The *Interpretative Guidance* distinguishes between civilians who take part in hostilities sporadically and those who are members of an organized armed group:

> Civilians lose protection against direct attack for the duration of each specific act amounting to direct participation in hostilities, whereas members of organized armed groups belonging to a non-State party to an armed conflict cease to be civilians […], and lose protection against direct attack, for as long as they assume their continuous combat function.[54]

The loss of protection for each specific act amounting to direct participation in hostilities, and its corollary, the regaining of the protection between each act, is generally called the *revolving door*. This *revolving door* is a controversial notion,[55] and in this way the *Interpretative Guidance* specifies that «[t]he «revolving door» of civilian protection is an integral part, not a malfunction, of IHL.»[56] The experts taking part in the *Tallinn Manual* process were divided on this issue and no consensus was found.[57]

The *revolving door* is something important that should not be abolished. I believe that it is, indeed, the best way to address the problem of civilians taking direct part in hostilities without giving a disproportionate advantage to either side. However, this notion seems to be very difficult to apply to civilians taking part through cyber means for two reasons. Firstly, cyber attacks can be very quick to launch and so the direct participation of the civilian seems to be difficult to address given the short duration span.

---

52 Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 16.

53 Ibid 37–38.; Israel, Supreme court, *Targeted Killing Case*, (note 93), § 38; ICTY, Appeals Chamber, *Blaškić* (Judgment), IT-95-14-A, 29 July 2004, § 157.

54 *Interpretive Guidance* (n 13) 17, 70.

55 Boothby (n 24) 753–759; Watkin (n 14) 686–690; Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 37–38; Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89, 102.

56 *Interpretive Guidance* (n 13) 70.

57 *The Tallinn Manual* (n 9) rule 35, § 10.

Secondly and especially, most cyber attacks are detected after their perpetration, when the civilian perpetrator has already regained his civilian protection.[58]

However, the purpose of the notion of direct participation in hostilities is not to punish the civilian who takes direct part, as a sanction for criminal behavior, «but a consequence of military necessity in the conduct of hostilities.»[59] At the end of his direct participation, a civilian regains his civilian protection and shall again enjoy general protection against dangers arising from military operations. But, this civilian does not enjoy immunity for his acts. Indeed, he remains «subject to criminal prosecution for violations of international or domestic law [he] may have committed during such participation».[60]

Based on this framework, it can be assumed that the difficulty highlighted just before, arising from the short duration of the cyber direct participation, perfectly aligns with the objective of the notion of direct participation that is to end the threat arising from the participation. The civilian remains subject to criminal law and shall be brought to justice for his acts. It is important to note that it is not the direct participation *per se* that is criminalized but the acts perpetrated by the civilian who has directly participated in hostilities.[61] Also, as explained later in this article, there are other ways to end the threat represented by a civilian taking direct part in hostilities through cyber means. It is the same for civilians who were members of an organized armed group and who have regained their civilian protection.

Contrarily, civilians who are «[m]embers of organized armed groups belonging to a non-state party to the conflict cease to be civilians for as long as they remain members by virtue of their continuous combat function.»[62] As a consequence, civilians who are assuming continuous combat function as members of an organized armed group, even if only through cyber means, lose their protection as long as they stay with this armed group and do not end their continuous combat function, and this applies not only for each cyber attack they perpetrate.

3.3. Presumption of non participation in case of doubt

According to article 50(1) of Protocol Additional I, «[i]n case of doubt whether a person is a civilian, that person shall be considered to be a civilian». Section VIII of

58 See e.g. Prescott (n 35) 258–259; Schmitt, 'Cyber Operations and the Jus in Bello' (n 55) 102.

59 *Interpretive Guidance* (n 13) 62.

60 Dieter Fleck, *The Handbook of International Humanitarian Law* (Oxford University Press 2007) 261, § 519.

61 *Interpretive Guidance* (n 13) 83–85.

62 Ibid 71.

the *Interpretative Guidance* extends this presumption to the determination of whether a civilian is taking direct part in hostilities.[63] Accordingly, when a person is considered to be a civilian, that person can belong in three different categories: civilians who are not taking part in hostilities, «civilians directly participating in hostilities on a spontaneous, sporadic, or unorganized basis», or members of organized armed groups.[64] If there is a doubt over whether that person has directly participated in hostilities, or whether that person is a member of an organized armed group, that person shall be considered to be a civilian not taking direct part in hostilities.[65] The experts taking part in the *Tallinn Manual* were split and did not find a consensus on the existence of this presumption.[66] The position of the ICRC expressed in the *Interpretative Guidance* is, from my point of view, the most accurate one.

3.4. Restraints on the use of force in direct attacks

Section IX of the *Interpretative Guidance* titled *Restraints on the use of force in direct attacks*[67] seems to be one of the most controversial.[68] As we will see below, this section is also one of the most interesting for the application of the notion of direct participation to cyber warfare.

The idea of this section can be found in the famous statement of Jean Pictet, who wrote that «[i]f we can put a soldier out of action by capturing him, we should not wound him; if we can obtain the same result by wounding him, we must not kill him.

63 Ibid 74–76.

64 Ibid 74.

65 Ibid 75–76; for some scholars '[t]here is no presumption that civilians are not directly participating', see e.g. Boothby (n 24) 766; for some other scholars, in case of doubt, civilian should be presumed to be directly participating in hostilities, see e.g. Michael N Schmitt, '«Direct Participation in Hostilities» and 21st Century Armed Conflict', *Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck* (2004) 509; see also Schmitt, 'Deconstructing Direct Participation in Hostilities' (n 3) 737–738; see also the reply from Nils Melzer to those criticisms: Melzer, 'Keeping the Balance Between Military Necessity and Humanity' (n 14) 857.

66 *The Tallinn Manual* (n 9) rule 35, § 12.

67 *Interpretive Guidance* (n 13) 77–82.

68 See e.g. Parks (n 14) *passim*; Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities' (n 8) 39–43; *contra* see Melzer, 'Keeping the Balance Between Military Necessity and Humanity' (n 14) 895–896 ('While Parks rightly points out that, during the expert discussions, several participating experts were extremely critical of Section IX, he fails to note that just as many experts strongly supported its inclusion in the Interpretive Guidance, and several others even argued that Section IX was not sufficiently restrictive, but should be complemented by human rights standards on the use of force.').

If there are two means to achieve the same military advantage, we must choose the one which causes the lesser evil».[69] In this way, this section means that «[i]n addition to the restraints imposed by international humanitarian law on specific means and methods of warfare, and without prejudice to further restrictions that may arise under other applicable branches of international law, the kind and degree of force which is permissible against persons not entitled to protection against direct attack must not exceed what is actually necessary to accomplish a legitimate military purpose in the prevailing circumstances.»[70]

Footnote 221 of the *Interpretative Guidance* delivers some interesting information for this article:

> During the expert meetings, it was generally recognized that the approach proposed by Pictet is unlikely to be operable in classic battlefield situations involving large-scale confrontations (report DPH 2006, pp. 75 f., 78) and that armed forces operating in situations of armed conflict, even if equipped with sophisticated weaponry and means of observation, may not always have the means or opportunity to capture rather than kill (report DPH 2006, p. 63).

I find this statement very interesting in light of cyber warfare. Indeed, in the confusion of a classic battlefield it can be difficult to adapt the force and the means of an attack to each civilian taking direct part in hostilities. However, the situation is different with cyber direct participation in two ways.

Firstly, those civilians are not on the battlefield, they are not directly and physically threatening soldiers by holding a weapon and targeting them. So there is no direct threat to the soldier that can lead to the necessity to shoot the civilian before he shoots the soldier.

Secondly, following Jean Pictet we can say that it is better to capture the civilian than to wound him, and it is better to wound him than to kill him. In the case of civilians directly participating through cyber means, there is another possibility: that is to target his way to access to cyberspace and to launch cyber attacks. Indeed, without his access to cyberspace (computer, network, or even is electricity access) this civilian is no longer a danger for the military. I think that this possibility is to be seen as equivalent to the option of capturing him, and is to be understood as better than wounding or killing him. However, this solution can be criticized in that the civilian can find another computer, or if the network is disabled, another way to access it and perpetrate cyber attacks. But this issue can be addressed easily by capturing the civilian at the same time in order to remove the cyber threat he represents.

---

69 *Interpretive Guidance* (n 13) 82, footnote 221.

70 Ibid 77.

4. A CHALLENGE FOR THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES AND CYBER WARFARE: THE APPLICATION *RATIONE LOCI* OF IHL AND THE SPATIAL LIMITS OF ARMED CONFLICTS

IHL is applicable solely in the context of an armed conflict.[71] As a consequence, IHL is only applicable in the geographical limits of the armed conflict. Mary E. O'Connell perfectly illustrates this in relation to the war in Afghanistan:

> In addition to exchange, intensity, and duration, armed conflicts have a spatial dimension. It is not the case that if there is an armed conflict in one state –for example, Afghanistan– that all the world is at war, or even that Afghanis and Americans are at war with each other all over the planet. Armed conflicts inevitably have a limited and identifiable territorial or spatial dimension because human beings who participate in armed conflict require territory in which to carry out intense, protracted, armed exchanges. International armed conflicts involving sovereign states inevitably implicate the territory controlled by those states,[72]

Civilian direct participation in hostilities is an IHL notion, and so, as a consequence, it is only relevant and applicable in the context of an international or non-international armed conflict. The ICRC's *Interpretative Guidance* mentions the problem of the evolution of means of warfare and the increasing ability to perpetrate attacks far away from the target.

> The requirement of direct causation refers to a degree of *causal* proximity, which should not be confused with the merely indicative elements of *temporal* or *geographic* proximity. For example, it has become quite common for parties to armed conflicts to conduct hostilities through delayed (i.e. temporally remote) weapons-systems, such as mines, booby- traps and timer-controlled devices, as well as through remote-controlled (i.e. geographically remote) missiles, unmanned aircraft and computer network attacks.[73]

We can identify three main evolutions in the way that civilians can directly participate in hostilities. The first one, the most simple, is the physical participation in the battlefield. Civilians take up weapons and fight the enemy physically.

The second one is the result of the use of vessels and drones by armies. Drones and vessels used for warfare are very expensive and difficult to access for civilians outside of the context of armies, and so those civilians are mostly taking direct part in hostilities from a localization encompassed in the geographical limits of the armed conflict. This situation was perfectly identified by Ryan Goodman and Derek Jinks:

> The concept of DPH has had to bear an especially heavy weight in contemporary armed conflicts. Technological developments have expanded the capacity of individuals to apply lethal

71 See e.g. Fleck (n 60) 45, § 201.

72 Mary Ellen O'Connell, 'Combatants and the Combat Zone' (2009) 43 University of Richmond Law Review 845, 858.

73 *Interpretive Guidance* (n 13) 55.

> force while remaining located thousands of miles away from their targets. States have increasingly relied on private contractors to maximize military power.[74]

The third and last evolution is cyber warfare and cyber means: civilians can take part in hostilities from everywhere in the world with great ease. This situation challenges the geographical limitation of the conflict as civilians can take part in hostilities from outside of the geographical limits of the armed conflict. As a consequence, those civilians can be located in a place where IHL, and *a fortiori* the notion of direct participation in hostilities, are not applicable.

On the geographical limitations of cyber operations, the *Tallinn Manual* notes:

> As a rule, cyber operations may be conducted from, on, or with effects in the entire territory of the parties to the conflict, international waters or airspace, and, subject to certain limitations, outer space. Cyber operations are generally prohibited elsewhere. Or particular importance in this regard is the law of neutrality because cyber operation can transit neutral territory and may have unintended effect therein.[75]

However, cyberspace offers the possibility for civilians to design and launch cyber attacks against belligerents from the territory of a State not involved in the armed conflict. During an armed conflict, only the cyber operations perpetrated by civilians within the geographical limits of the armed conflict and of the application of IHL, can be regarded as direct participation in hostilities. However, civilians located outside of the geographical limits of the armed conflict can perpetrate cyber operations that reach the three cumulative criteria of DPH identified by the ICRC, namely the threshold of harm, a direct causation and the belligerent nexus. What about those civilians? Are they immune from prosecution for their acts?

Clearly, the answer is no. Civilians taking part in hostilities from outside the geographical limits of the armed conflict cannot be qualified as taking direct part under IHL but they can be prosecuted for their acts. Applying the notion of direct participation to all civilians taking part from outside of the geographical limits of the armed conflict would lead to extrajudicial killing of civilians that must not become the way of addressing this issue.[76]

Targeted States cannot act directly against those persons. These States must ask the State from which the cyber operation came to prosecute the civilian perpetrator. This situation leads to a practical critique: this procedure can be long, and during this time the civilian can continue his cyber operation. The hosting States may also be uncooperative.

---

74 Ryan Goodman and Derek Jinks, 'ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum, The' (2009) 42 New York University Journal of International Law and Politics 637.

75 *The Tallinn Manual* (n 9) rule 21, § 1.

76 Goodman and Jinks (n 74) 639.

In the previous paragraphs, I have described briefly the legal framework of the spatial scope of the application of IHL and the notion of direct participation in hostilities. I will not go further in this reflection at this point, although it is safe to state that the issue deserves further and broader analysis on how cyber warfare is challenging the *ratione loci* application of international law.

However I will describe here a few short reflections on this issue. Firstly, nowadays, States are trying in different ways to address the various situations challenging this spatial limitation of armed conflict. The best example seems to be the United States and the global 'war on terror', notably though the use of drones for targeted killing in States with which the United States is not engaged in an armed conflict. Several theories have been developed and used in this way, for example the 'unwilling or unable' States or the notion of 'transnational armed conflict'; those notions are far from being fully accepted and uncontroversial under international law and by the international community. It will be very interesting to compare those notions to cyber warfare. Nonetheless, cyber warfare differs a lot from the existing battlefields. If we analyze the two situations from a practical, and not legal, stand point, it must be highlighted that targeted killings usually take place in States close to the battlefield, but not parties to the armed conflict, and often those States are qualified as 'unable or unwilling' to act against the threat. Conversely, the use of computer technology allows people to take part in hostilities from all around the world, even very far from the targeted States, and in States where it seems more difficult to violate their sovereignty without consequence.

For example, what if someone in France designed a cyber operation against Israel, in support of the Hamas or the Hezbollah, in their conflicts with Israel? Even if the operation perpetrates by this person located in France reached all the criteria of the direct participation in hostilities, it seems impossible to qualify it as direct participation under IHL as the perpetrator is not located within the spatial limits of the armed conflict. The only solution for Israel would be to ask France to act against this person, and if France refused it would be difficult, or even impossible and dangerous, for Israel to use the 'unable or unwilling' State theory against this person within the French territoryThis distinction between those who take part within the geographical limits of the armed conflict and those who act from outside is particularly relevant in cyber warfare. Here we can analyze the conduct of people on the Internet and notably those who claim to be part of the group Anonymous. Regularly, people from all around the world, acting on the behalf of Anonymous, are taking direct part in different armed conflict (e.g. the Israeli-Arab conflict or the conflict between the two Koreas). In light of the previous development, it seems that most of these actions cannot be qualified as direct participation in hostilities under IHL and can be solely addressed under law enforcement procedure.

5. THE PARTICIPATION IN HOSTILITIES OF UNAWARE CIVILIANS

Internet makes it possible to work remotely, in collaboration with people all around the world. Thus, people involved in a cyber operation can be unaware of the final or real purpose of the operation and of their work. In cyber criminality, it is common to recruit people though the Internet with tempting offers to make money easily, without meeting them face-to-face and without them knowing the real purpose of this job. These people are usually totally unaware that they have become involved in a complex and illegal action that can lead them to prosecution under criminal law.[77] Then this way of involving people can, it might be assumed, be transposed to cyber warfare.

Surfing on the Internet, it is easy to find on blogs or forums people asking for help in order to develop computer codes or even to be involved in cyber operations. But, it is less easy to discover what will be the real use and consequences of your participation, and one could thus easily be unwittingly involved in cyber warfare. Internet is a collaborative world and this situation –giving help on a forum without knowing the real purpose of what we do– is very common.

The ICRC's *Interpretative Guidance* distinguishes the belligerent nexus from the subjective intent of the civilian who takes direct part in hostilities. However, it specifies that

> Only in exceptional situations could the mental state of civilians call into question the belligerent nexus of their conduct. This scenario could occur, most notably, when civilians are totally unaware of the role they are playing in the conduct of hostilities (e.g. a driver unaware that he is transporting a remote-controlled bomb) […]. Civilians in such extreme circumstances cannot be regarded as performing an action (i.e. as doing something) in any meaningful sense and, therefore, remain protected against direct attack despite the belligerent nexus of the military operation in which they are being instrumentalized. As a result, these civilians would have to be taken into account in the proportionality assessment during any military operation likely to inflict incidental harm on them.[78]

In the light of this, the possible situations described above cannot lead to the qualification of civilian direct participation in hostilities. Nonetheless, it seems very difficult to prove the civilian's awareness, or lack of awareness, or not of the final purpose of the cyber operation in which he is involved. As stated before in this article, if there is doubt as to whether a civilian is taking direct part in hostilities or not, this person shall be considered to be a civilian not taking direct part in hostilities.

Another issue arising from cyber warfare is the question of the use of the computer without the civilian owner knowing it, or against his or her will. Indeed, many cyber

77 See notably the TV documentary Dorina Herbst, *In Den Fängen Der Internet-Mafia* (Arte 2013).

78 *Interpretive Guidance* (n 13) 60.

operations used one or more botnets, which is a collection of compromised computers named bots. Such compromised computers have usually been infected by a malware that allows someone to use and control them remotely without the knowledge of their owners or users. In this situation, the owners of the compromised computers cannot be seen as taking direct part in hostilities. However, this situation raises many questions on the difficult dissociation between the owner, the user and the computer and their legal qualifications.

In sum, the notion of direct participation is challenged by cyber warfare but remains applicable. The practice will need to find how to address and fix the specific issues concerning civilian direct participation in hostilities in relation to cyber warfare.

6. CONCLUSION

This article demonstrates that IHL applies and is sufficient in most of cases of civilian direct participation in cyber hostilities. It proves, consequently, that the assertion according to which cyber warfare is not controlled by international law is wrong. In some specific cases, however, there is a need of a new interpretation or creation of IHL rules as demonstrated in this article.

By analyzing together the divergent approaches of the ICRC's *Interpretative Guidance* and the *Tallinn Manual*, this article highlighted the diversity of possible approaches.

7. BIBLIOGRAPHY

Boothby B, 'And for Such Time as: The Time Dimension to Direct Participation in Hostilities' (2009) 42 New York University Journal of International Law and Politics 741.

Dinniss HH, *Cyber Warfare and the Laws of War* (Cambridge Studies in International and Comparative Law, Cambridge University Press 2012).

Doswald-Beck L and Henckaerts J-M, *Customary International Humanitarian Law: Volume 1, Rules.* (2004).

Fleck D, *The Handbook of International Humanitarian Law* (Oxford University Press 2007).

Goodman R and Jinks D, 'ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum, The' (2009) 42 New York University Journal of International Law and Politics 637.

Herbst D, *In Den Fängen Der Internet-Mafia* (Arte 2013).

Kerschischnig G, *Cyberthreats and International Law* (Eleven International Publishing 2012).

Melzer N, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross, 2009).

—, 'Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities' (2009) 42 New York University Journal of International Law and Politics 831.

—, 'Civilian Participation in Armed Conflict' [2010] Max Planck Encyclopedia of Public International Law.

O'Connell ME, 'Combatants and the Combat Zone' (2009) 43 University of Richmond Law Review 845.

Parks WH, 'Part IX of the ICRC Direct Participation in Hostilities Study: No Mandate, No Expertise, and Legally Incorrect' (2009) 42 New York University Journal of International Law and Politics 769.

Prescott JM, 'Direct Participation in Cyber Hostilities: Terms of Reference for like-Minded States?', *2012 4th International Conference on Cyber Conflict (CYCON)* (2012).

Schmitt C, *Theory of the Partisan: Intermediate Commentary on the Concept of the Political* (first published 1963, translated by G L Ulmen, Telos Press Publishing 2007).

Schmitt MN, '«Direct Participation in Hostilities» and 21st Century Armed Conflict', *Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck* (2004).

—, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42 New York University Journal of International Law and Politics 697.

—, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 Harvard National Security Journal 5.

—, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89.

— (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

Watkin K, 'Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretive Guidance' (2009) 42 New York University Journal of International Law and Politics 641.

Watts S, 'Combatant Status and Computer Network Attacks' (2010) 50 Virginia Journal of International Law 391.

TOWARDS A MAGNA CARTA FOR THE INTERNET: A RIGHT TO ONLINE PROTESTS?

Argyro P. Karanasiou
Lecturer in Law
(Centre for Intellectual Property Policy & Management)
Bournemouth University, UK

ABSTRACT: The paper examines the changing face of protesting in the digital era with a particular focus on DDoS attacks. While it is generally recognized that new technologies and the Internet have played a seminal part in mobilizing the masses, the issue of online protesting is highly overlooked in the literature. The paper highlights the Internet's contribution to the organization of major protesting movements, such as the Spanish Indignados but takes a further look on it serving as an environment for online protesting. An initial taxonomy of potential online demonstrations is followed by a legal assessment of DDoS as protesting acts. The latter has been an attractive argument claimed many times by the Anonymous hacking collective, most notably on January 2013 in a White House petition suggesting that DDoS[1] attacks ought to be recognized as a valid form of protest, similar to the Occupy movements. This paper examines the analogies between offline protests and DDoS attacks, discusses legal responses in both cases and seeks to explore the scope for free speech protection[2].

KEYWORDS: DDoS, free speech, digital sit-in, civil rights movement, protest.

1. A MAGNA CARTA FOR THE INTERNET: TOWARDS A RIGHT TO OCCUPY CYBERSPACE?

In March 2014, marking the 25th anniversary of the World Wide Web, sir Tim Berners Lee called for a Magna Carta Bill of Rights for the Internet users and described this as a communal decision in the public interest. Following up on this, the «Web We Want» campaign has been added to a long list of advocacy groups and legal scholars urging for the need of drafting a charter of fundamental human rights online. Most notably, the Charter of Human Rights and Principles for the Internet and the related 10 Rights and Principles for Internet governance are initiatives developed by the Internet Rights and Principles Dynamic Coalition (IRP) that outline a list of rights for users. Article 7 of the IRP Charter suggests

1 Distributed Denial of Service attacks, thereafter referred to as DDoS

2 A previous version of this has appeared in the International Review of Law Computers & Technology (2014). All errors and omissions remain the sole responsibility of the corresponding author.

a right for online assembly and association in noting that «Everyone has the right to form, join, meet or visit the website or network of an assembly, group or association for any reason. Access to assemblies and associations using ICTs must not be blocked or filtered».

It is generally argued that the Internet serves as a global platform, where different groups of interests can come together, interact and communicate. As such, internet access is closely related to one's right to assemble online. Yet, could this also further suggest one's right to protest online?

The internet's contribution to mass mobilisation serving as a communicatory platform that can facilitate protesting acts has been noted on many occasions: The Greek protests in 2008 presented a unique case of spontaneous youth mobilization, which was organized mainly through the use of the internet and mobile phones, had no political interference in its organizational frame and yet managed to convey a political message for the urgent need to deconstruct the current status quo and demanded radical social change[3]. In a similar manner the Spanish 'Indignants' protests and the Occupy movements in various public places all over the word have all been cases of nonviolent sit-ins protesting against financial inequality and wealth disparity[4] facilitated at large by online social networking sites [5]. In spite of their different foci, these protests have all followed a similar pattern of 'sit-in demonstrations' for organizing their protesting activities: encampments were set up occupying squares and public places, where people had the opportunity to deliberate, transfer knowledge and exchange ideas, personal concerns and information. At the same time, another form of contemporary protesting has emerged lately: online protests illustrate that the internet besides a medium can also be a different playing field altogether hosting a number of alleged «digital sit-ins». Distributed-Denial-of-Service attacks, widely known as DDoS, are believed by many to be one such case of online civil-disobedience[6]. A criminal assault in most jurisdictions, DDoS attacks artificially create heavy traffic flow for a website rendering its services temporarily inaccessible. In a way DDoS seem to operate in the same manner that the 'Occupy' protests do: occupation is used as a means of getting a message across. Yet, are DDoS attacks occupying cyberspace, the same way protestors in the occupy movements occupied public spaces and squares to promote their causes? This paper will examine whether DDoS are indeed the digital counterpart to sit-ins and whether they could further qualify as free speech meriting constitutional protection.

---

3 For more see (Psimitis 2011); (Sakellaropoulos 2012); (Sotiris 2010)

4 For a note on the causes that protestors in the occupy movements are seeking to promote through their actions, see (Doyston 2012) 20-24

5 This is clearly illustrated in the report by N Caren, S Gaby, «Occupy Online: Facebook and the Spread of Occupy Wall Street» (October 24, 2011). Available at SSRN: http://ssrn.com/abstract=1943168

6 See for example (Morozov 2011) 227-229

2. INSTANCES OF ONLINE PROTESTING: A NO SIZE FITS ALL APPROACH

The fact that the repertoire[7] of collective actions has gained new dimensions online is so widely acknowledged in many scholarly papers[8] in the field of social sciences that it makes it hardly necessary to elaborate on the matter further. That said whether there is scope for DDoS attacks to be granted free speech protection is a question that cannot be answered by drawing a simple analogy. This would be a risky proposition.

The various ways in which 'hacktivism' and virtual protesting operate as a whole leave ample authority for the proposition that not all cases of online protesting are alike. This point is very well illustrated when reviewing notable cases of online protests. As it shall become obvious in the remainder of this paper, it is almost impossible to legally assess one's right to online protest without distinguishing between the causes, all means and methods employed their participatory levels and organisational structure of such acts. The following examples can be adduced:

2.1. Digital Zapatistas

One of the first documented cases of DDoS are the 1998 attacks launched by the online collective Electronic Disturbance Theatre (EDT) against the websites of the White House and the Mexican's president Zedillo[9]. Using Netflood software, which overwhelms a website with bad requests, the EDT sought to block these websites as a means of protest for paramilitary practises against indigenous in Chiapas. The EDT's co-founder, Ricardo Dominguez considers these attacks as acts of civil disobedience, equivalent to a digital sit-in, fitting the Rawlsian description of sit-ins[10].

2.2. Operation Payback

This case furnishes a great example of 'hacktivism' as it transposes the methods and motives behind a typical Anonymous 'operation'. Following the WikiLeaks cable leak in 2010, the internet activist group Anonymous launched DDoS against websites of banks who had stopped providing services to WikiLeaks due to political pressure. WikiLeaks

7 For a general introduction to the «repertoire of collective action» see (Tilly 1984) 297-317.

8 For more see (Ayres 2003) 132-143; (J Clark and Themudo 2003) 109-126; (Costanza-Schock 2003) 173-191; (Diani 2000) 386-401; (Garrett 2006) 202-224; (Rheingold 1993); (J Van Laer and Aelst 2010) 1-26; (W Van De Donk et al. 2004)

9 (Dominguez 2009)1806-1812. See also, (Lane 2003)129-144

10 (Rawls 1996) 356

neither applauded nor condemned the attacks[11]; however they did deny any connection to this activity.

2.3. Webzin

Another method of overloading a server as means of a digital protest, yet different from DDoS attacks altogether, is the case of email-bombing. In July 2001 an Australian labour organization managed to organize such an online protest against the legislation on worker's compensation by encouraging all participants to email the government. In this case, contrary to DDoS, there was no software used, however the result was equally disruptive as 13.000 emails were sent[12].

2.4. Virtual protest in second life

A slightly different case of digital protest is the online strike against IBM taking place in Second Life in 2007[13]. After the contract negotiations between RSU[14], a large European Labour Union and IBM reached a dead end, RSU staged the first virtual strike taking place in Second Life, an online virtual community. By running training courses and uploading relevant material, RSU provided information regarding the planned strike and the ways to construct a virtual persona in Second Life for all potentially interested participants. On September 2007 the first virtual protest took place online with the participation of protestors from over 30 countries; one month later the IBM Italy CEO handed in his resignation and a new contract was agreed.

All of the above selected cases of digital protests suggest that it would be wrong to treat DDoS as another type of online protest. Instead we should direct our attention to the specific features in DDoS attacks that distinguish them to other cases. Next follows a brief account of the main methods employed to orchestrate a DDoS attack as well as their key features.

3. HOW DO DDOS ACTUALLY OPERATE? TECHNICAL ASPECTS AND MAIN FEATURES

The Broughton suspension bridge in Salford, Greater Manchester furnishes us with an excellent example as to how DDoS attacks work. On 12 April 1831 the bridge co-

11 http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/wikileaks-refuses-to-back-condemn-anonymous-attacks-10021275/, accessed 2/5/2012

12 (Meikle 2002) 163

13 (B Blodgett) available at http://aisle.aisnet.org/amcis2010/553, accessed 3/5/2012

14 RSU stands for Rapressentanza Sindacale Unitaria

llapsed as a result of resonance caused by a unit of soldiers crossing the bridge in step[15]. The synchronized marching that the soldiers maintained is believed to have played an important role in the destruction of the bridge: in mechanics and construction engineering such synchronized vibrations tend to cause resonance, namely the phenomenon of increased oscillation that matches the frequency of the system's natural vibrations causing it to absorb more energy and to ultimately collapse. To avoid this soldiers are nowadays trained to break cadence when marching over bridges.

DDoS operate on a similar pattern: their result relies on the orchestrated actions of users en masse. Distribution is the main feature of this kind of web attacks: An overload of requests for information is sent at the same time to the web-server under attack from various distributed non-users. To complicate things further, these requests can also be generated automatically by a remotely controlled botnet, namely a coordinated network of software programs which perform an automated process[16]. In doing so these attacks seek to create false traffic, saturate the network's available resources and to ultimately disrupt its normal function by making it unavailable for its actual users[17].

There are many techniques to overload a system's server, all of which seem to be exploiting the net infrastructure and the way in which communication between computers is set out[18]. One point is worth noting here: Regardless of the specific technique used to launch a series of DDoS attacks, their function is based most of the times on exploiting the basic elements of the net infrastructure. Namely, to generate a series of DDoS attacks one would need to instruct simultaneous commands to be carried out by a great number of computers, all connected to the targeted server. The internet architecture is largely based on many interconnected machines communicating and exchanging information: DDoS operate by using such conceptual elements of the net infrastructure to achieve their goal, namely to overwhelm the targeted server deeming it unable to communicate.

This observation helps us further to identify the main features of the DDoS attacks, which could be summarized in the following three key points: Massive participation,

15 (R Taylor and Phillips 1831) 384-389

16 For more on this see (Chandler 2003-2004)

17 http://whatismyipaddress.com/DDOS-attack

18 A detailed account of all possible cases of DDoS would be more suitable to a paper focusing on the taxonomy of DDoS attacks and as such it would not add to the paper's purpose, which is the legal evaluation of DDoS as forms of protest. Thus, I refrain myself from the task of additional technical details and refer the reader to relevant bibliography. For a general overview see «DDOS Basics», Team Cymru Whitepapers March 2010, available online at http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/DDOS-basics.pdf, accessed 3/5/2012. See also (E Sinrod and Reilly 2000) 189-203

disruption of communication[19] and exploitation of the security holes of the server and the general way communication is set out by the net infrastructure[20]: the core net principles of trust between peers, distributed control and interdependent security make the internet exploitable to DDoS.

4. DDOS AS AN ACT OF CIVIL DISOBEDIENCE? A PHILOSOPHICAL INQUIRY

It has often been suggested that DDoS are to be perceived as another form of online civil disobedience. Yochai Benkler has recently described the 'Anonymous' online network group, known for its wide use of DDoS attacks, as a sit-in by design causing disruption and not destruction[21].

Contrary to what Benkler describes as a digital sit-in, there is also the view that DDoS should be approached with more scepticism at to their impact, methods and purposes. According to this view[22] DDoS do not qualify as a form of acceptable civil disobedience for two reasons: the low personal cost assumed by the participants and their operating routine, which is predominantly an attack against data-flow. The relatively easy participation to DDoS attacks, which does not incur any significant personal cost for the participants, is actually responsible for stripping these acts of one of the main components of civil disobedience: the element of public act. Namely, such online attacks lack the public quality of normal acts of civil disobedience, since the latter are meant to make a statement through the risk incurred for their participants. This type of online activism by simply contributing with a few clicks from the safety of home is described as 'slacktivism'[23], namely a «feel good online activism that has zero political or social impact»[24]. Second, it is highly unlikely that DDoS could be regarded as an act of non-violent civil disobedience meriting the constitutional protection of the right to

19 For example malware or viruses downloaded on their personal computer

20 (J Mirkovic and Reiher 2004) 40

21 Y Benkler «Hacks of Valor: Why Anonymous is Not a Threat to National Security», Foreign Affairs, available online at http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor., accessed 3/5/2012. For a similar view see also (Klang 2004b)

22 Tom Watson «Denial of Service, Denial of Speech», available online at http://tomwatson.typepad.com/tom watson/2010/12/denial-of-service-denial-of-speech.htm, accessed 3/5/2012

23 See (Gladwell and Shirky 2011) arguing that social movements in general are not made possible just by utilizing online media. On the other side of this debate, there are also theorists who believe in the great power social media in general have to mobilise the masses and to bring about social change (Castells 2012). For a good account on the relevant debate see (Fuchs 2012).

24 (Morozov 2010)

free speech as they themselves are inhibiting free speech[25], regardless of the legitimacy or nobility of their cause. It is true that granting free speech protection to DDoS would be contradictory as it would sanctify acts that seek to impede free speech by labelling them as constitutionally protected speech.

Denning introduces three main categories of online social movements: activism, 'hacktivism' and 'cyberterrorism'[26]. Whereas online activism is largely a non-violent computer mediated means of protest[27], 'hacktivism' and 'cyber-terrorism' suggest disruptive and thus illegal uses of computers. 'Hacktivism' in particular relies on

> «the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development»[28].

As such, 'hacktivism' is found to be consistent with the philosophy of civil disobedience[29], whose acts are illegal by definition and employ non-violent methods to restore the injustices encountered in law[30]. We could therefore draw the conclusion that DDoS are indeed to be regarded as a type of online civil disobedience. To suggest however that all virtual protests are instantiations of online civil disobedience would be an unjustified generalization, which can hopefully be refuted.

On the other hand, one can consider that DDoS are somehow less risky than other cases of civil disobedience, as, for example these attacks often simply involve downloading a certain piece of software, without requiring extra efforts to join them. Although, DDoS attacks include a fair degree of accountability and personal costs[31]

---

25 O Ruffin from the hacktivist collective CDC has stressed the oxymoron of curtailing free speech as a method of promoting free speech. For more see, (Atton 2004) 22

26 (Denning 2001)

27 For more see (M Mcaughey and Ayers 2003)

28 (Samuel 2004)

29 (Marion and Goodrum 2000);(Wray 1998) 107-111.

30 For an interesting comparison between the philosophies underpinning civil disobedience and online civil disobedience acts, mostly undertaken by the online collective of electro hippies see (Klang 2004a) 2

31 Note for example the electrohippies collective stating that their identities are easily traceable online as they do not use encrypted methods of communication. DJNZ and the Action Tool Development Group in «Client Sided Distributed Denial of Service: Valid Campaign Tactic or Terrorism Act?» Electro hippie collective, occasional paper 1, pp 8-9, available online at http://www.iwar.org.uk/hackers/resources/electrohippies-collective/op1.pdf, accessed 3/5/2012. See also J Bonneau, who argues that the hypothetical case of participants giving up their online identities would add to the commitment, rigor and legitimacy of DDOS as it would entail this missing element of personal sacrifice. J Bonneau, *Digital immolation*: *New Directions* in *Online Protest,* Eighteenth International Workshop on Security Protocols. Cambridge, UK, Mar 25

[32], this might still not be sufficient to render DDoS equivalent with civil disobedience offline.

These often low personal costs entailed, taken together with the weak ties noticed between the participants and the adversarial nature of DDoS attacks also seem to suggest that these attacks are exemplar cases of what Van Laer and Van Aelst would call internet based action with low participatory threshold: in the context of their «new digitalized action repertoire»[33]. DDoS attacks are exemplar cases of internet based as opposed to internet supported online collective actions[34].

That said, participation to DDoS attacks does not presuppose a high level of expertise in hacking techniques[35]. Take for example the Low Orbit Ion Cannon (LOIC) used in the 'Anonymous' DDoS attacks. LOIC is an application developed by hackers which when activated renders control of the computer to a central Anon Administrator to reload a targeted website, generate a great number of requests and to ultimately overwhelm the website causing it to crash[36]. In a way this could be described as willingly rendering authorisation to a hacker to take control of a computer's network connection. The low risk a LOIC user runs[37] combined with the ease of participating by simply downloading this application has resulted from its wide use[38].

As such, participation to the Anonymous DDoS attacks has a lower threshold compared to offline acts of civil disobedience. Thus, the analogy of DDoS attacks to acts of

2010, available online at http://www.cl.cam.ac.uk/~jcb82/doc/B10-SPW-online_protest.pdf , accessed 3/5/2012

32 Meikle refers to such potential risks mentioned by the Electronic Disturbance Theater, an online collective staging the virtual sit-in for the raising awareness on the Zapatistas movement in Mexico: «This is a protest, not a game, it may have personal consequences as in any off-line political manifestation on the street» (Meikle 2002) 144

33 (J Van Laer and Aelst 2010) 230-254

34 An internet supported action with low participatory threshold is for example an online donation whereas an example of the same action with high participatory threshold is the organization of transnational social movements such as the world social forum.

35 (Yar 2006) 32

36 What is LOIC? Available online at http://gizmondo.com/5709630/what-is-loic, accessed 2/6/2012. For a brief account on how Anonymous launch their DDOS attacks by distributing links to web-based versions of LOIC see A Chen, «The Evil New Tactic Behind Anonymous' Massive Megaupload Revenge Attack», available online at http://gawker.com/5877707/the-evil-new-tactic-behind-anonymous-massive-revenge-attack, accessed 3/5/2012

37 ibid

38 It has been estimated that LOIC was downloaded 27,686 times on December 9th 2010 during the Anonymous «Operation Payback», namely the multiple DDoS attacks against Amazon, PayPal, MasterCard, Visa and the Swiss BankPostFinance in support to WikiLeaks.

civil disobedience would be an oversimplified assumption, which does not seem to be correct.

5. DDoS AS AN ACT OF PROTEST MERITING FREE SPEECH PROTECTION?

In the previous section it was shown that DDoS attacks seem to share some common traits with acts of civil disobedience; however their technical aspects and participatory standards would not allow for a direct analogy to sit-ins. The remainder of the paper will consider the general argument that such an analogy suggests: DDoS as a protesting act meriting free speech protection. This argument has been used time and again for the legal defence used in cases of arrested hackers involved in DDoS attacks. It is of course no coincidence that such an argument has been put forward in the US, where First Amendment protection is frequently sought to avoid the distressing application of the law of such cases as those under review here. The First Amendment doctrine embodies principles that forbid the abridgement not only of speech but also of conduct[39]. If the conduct under review is found to convey a political message, it falls within the remit of political speech, and as such it is granted First Amendment protection.

In the case of DDoS attacks presented as the digital equivalent of a sit-in, it is important to examine carefully the relevant case law. In tracing any analogies between protected acts of protests and DDoS[40], a new understanding of the right to protest in the digital era is sought to be established.

5.1. DDoS as protected acts of public protest: Equality

Before anything else, it would be useful to revisit the granted protection on similar cases in the past, to configure the main argument underpinning the free speech jurisprudence and to ultimately discuss whether this would also be applicable in the case of DDoS. An appropriate point of reference for this would be the categorisation of the various acts of public protest offered by Helen Fenwick. According to their specific traits and their level of violence, acts of public protest can be grouped in the following categories: «peaceful persuasion, offensive or insulting persuasion, intimidation, symbolic or persuasive physical obstruction or interference, actual physical obstruction or interference, forceful physical obstruction and violence»[41].

39 See (Nimmer 1973) 61-62

40 See also (McLaurin 2011) 239-246 for an excellent analysis on the comparison between DDoS and civil rights movements.

41 (Fenwick 1999) 494

DDoS seem to be falling in the remit of a persuasive interference as they seem to be combining both interference, as well as the intention to convey a message through this act. The judges in such cases are willing to accept the illegality of the act under review and to grant free speech protection should they find the act of protest has resorted to obstruction as a means of gaining publicity and getting a message across, which would otherwise have been impossible.

DDoS involve direct action in order to draw public attention to a cause and appear to be both obstructive and persuasive in the sense that it seeks to gain publicity and convey a message to the public by overloading a targeted website. The reason for protecting such obstructive acts, as Fenwick explains, is equality. Minorities and marginalized groups, whose causes are often poorly represented in the media, should be granted a certain level of free speech protection even at the expense of the rights of others[42]. One could claim that DDoS is very similar to such acts and argue that there might be room for manoeuvre in asking for free speech protection on grounds of equality. In the US, the relevant case-law seems to favour free speech protection for minorities: In the words of Justice Black, this is «essential to the poorly financed causes of little people»[43]. Justice Brennan quoting Justice Black[44] in his dissent in FTC v. Superior Court Trial Lawyers Association stated that «Expressive boycotts are irreplaceable as a means of communication because they are essential to the 'poorly financed causes of the little people'. It is no accident that boycotts were used by the American colonists to throw off the British yoke and by the oppressed to assert their civil rights»[45]. In summary, the right to free speech on equal grounds for all, even those with unpopular views, has always been of primary importance for the First Amendment. Would this suffice for recognizing DDoS as free speech?

5.2. DDoS as tresspassory assemblies

The analogy of DDoS to the Occupy Movements has already been discussed in previous sections of this paper. However, even if we accept that DDoS are similar to the tresspassory assemblies in the Occupy Movements, their balance to the protection of the occupied private property would still need to be decided. In 'occupying' a website,

42 For the Government's response to such direct acts of protest and for a commentary on the relevant UK stance on this matter see (Fenwick 2002, 3rd edition) 427-430

43 Martin v. City of Struthers, 319 U.S. 141, 146 (1943)

44 Justice Black's ruling has been rather influential and has been quoted in a number of other similar cases. See for example Justice Black dissenting «Access to government property permits the use of the less costly means of communication so 'essential to the poorly financed causes of little people'» Cornelius v NAACP Legal Def. & Educ. Fund, Inc., 473 U.S. 788, 815 (1985)

45 FTC v. Superior Court Trial Lawyers Association, 493 U.S. 411, 451 (1990)

DDoS attacks cause serious disruptions to the website's traffic; to what extent are such disruptions justified is what this section looks at.

Spatiality and property online have been discussed extensively[46] and I will not focus on them here; let us just agree that DDoS can be considered as tresspassory assembly as seemingly implied by section 3 of the UK Computer Misuse Act 1990[47], which criminalised all acts of interfering with a computer knowingly without authorisation[48]. In determining the balance between free speech and individual property the UK legal response to such questions has always focussed on the law of trespass[49]. The Public Order Act 1986 defines public forum in terms of expressed or implied permission for public access, which might lead one to think that DDoS are actually not an unauthorised act, as the main purpose of a website lies in the very fact of accepting online visitors. This point has been actually argued by the defendant in DPP v Lennon[50], the first reported DDoS conviction in the UK concerning a case of mass emails. Although this argument initially convinced the court to dismiss all charges for the defendant, Lord Justice Keene and Justice Jack allowed an appeal, stating that there was no implied consent «from the fact that the server has an open as opposed to a restricted configuration».[51] Thus it is clear that DDoS as a criminally proscribed act suggests trespass and as such it does not qualify for free speech protection in the UK[52].

In the US First Amendment protection for DDoS attacks is also hard to obtain: if the targeted website is considered private property First Amendment protection simply does not apply. In cases where public protests occur on certain private properties, which are symbolic and essential for drawing attention and conveying a message, the First Amendment protects these acts unless there are ample alternatives for gaining wide

46 (Burk 2000); (Epstein 2003); (Grimmelman 2010)

47 Added by section 36 of the Police and Justice Act 2006

48 For a good account on the UK legal responses to DoS and DDoS see (Edwards 2004) 23-62

49 (Clayton 2000) 252-260

50 DPP v Lennon [2005] EWCA Crim 2150. In this case, the court initially ruled that DDOS were not covered by the Computer Misuse Act, as it was not an unauthorised act. This was however overturned on appeal and resulted to the addition of sections 33-36 of the Police and Justice Act 2006 to broaden the scope of the Computer Misuse Act so as to include DDOS as well. For a good account of the UK legislative framework on the matter and its evolution, see (Fafinski 2008) 53; (Rachman 2012) 85-100

51 DPP v Lennon [*2006*] *EWHC 1201* (Admin), [2006] All ER (D) 147 at [14]

52 On a further note, it is likely that DDOS would also not fall within the protective scope of art 10 ECHR. The ECtHR has in certain cases accepted that restrictions of peaceful yet obstructive protests can be disproportionate (*Steel and Others v United Kingdom* (1998) 28 EHRR 603), yet it is doubtful whether DDOS could be seen as a type of peaceful protest.

attention[53]. In this vein, it has been ruled that boycotting[54], picketing near schools[55] or outside abortion clinics[56] are cases falling within the protective scope of the First Amendment. However, if we are to consider DDoS as an act of civil disobedience, acute to civil rights movements and sit-ins, it should be noted that «violent conduct is beyond the pale of constitutional protection»[57]. Namely, in cases of civil rights movements, although it is generally recognized that sit-ins are a powerful method of communication and protest[58] –which should not be restricted simply because it occurs on private property– such acts do not enjoy absolute free speech protection at the expense of private property.

In brief, DDoS are punishable acts of computer misuses, which are of tresspassory nature[59]. On the other hand, if we examined the matter beyond the concepts of spatiality and proprietorship of online websites could DDoS remain within the First amendment's protective scope? At a first glance, one could argue that DDoS could be permitted as expressive conduct in semi-private places. In Robins v Prune Yard Shopping Center[60], the California Supreme Court held that shopping malls constituted an invaluable forum for exercising free speech, as they were freely accessible by the public[61]. Could DDoS be justified along these lines on the understanding that targeted websites are openly accessible online? It has been argued that pure DDoS attacks caused by sending non malformed standard data packets are not an act of illegal access to a website but an action allowed by the system itself[62]. Hence, such actions could not constitute trespass. That said one should further consider the potential threat DDoS attacks pose to online free speech, discussed next.

---

53 Hill v. Colorado, 530 U.S. 703 (2000)

54 NAACP v. Claiborne Hardware Co., *458 U.S.* 886 (1982)

55 Police Department v. Mosely, 408 U.S. 92 (1972)

56 Madsen v. Women's Health Center, 512 U.S. 753 (1994)

57 NAACP v. Claiborne Hardware Co., *458 U.S.* 886, *933-34* (1982)

58 «Concerted action is a powerful weapon. History teaches that special dangers are associated with conspiratorial activity. And yet one of the foundations of our society is the right of individuals to combine with other persons in pursuit of a common goal by lawful means.» NAACP v. Claiborne Hardware Co., *458 U.S.* 886, *933-34* (1982)

59 S Kreimer offers a detailed overview of the US literature on the link between DDOS and common law of trespass (Kreimer 2001)

60 592 P. 2d 341 (Cal. 1979)

61 Note however that the US Supreme Court upheld the California court's decision while it also allowed for certain content neutral restrictions. Prune Yard Shopping Center v Robins, 447 U.S. 74 (1980). See also (Epstein 1997) 21–56.

62 http://forums.theregister.co.uk/forum/1/2012/02/08/DDoS_attack_trends, accessed 3/5/2012

5.3. DDoS and the slippery slope of free speech restriction

It has now hopefully been demonstrated that reviewing DDoS as a digital sit-in, would not stand many chances of success for gaining free speech protection[63]. In any case, it is generally understood that under no jurisdiction are public protests immune to total restriction, especially when there is the danger for a breach of peace to occur.

Be that as it may, free speech protection for DDoS would also be problematic in terms of proportionality. For if we were to declare that DDoS merits constitutional protection as free speech, at the same time we would meet with the most emphatic contradiction:

As DDoS is nothing but a tool destined to cause disruption, it has also been frequently associated with attacks to human rights and media sites resulting to online censorship of their content. However, there are other numerous cases reported of DDoS used as cyber censorship tools[64] while also the purposes of launching DDoS attacks against a website are not always related to public protest[65].

It is therefore clear that DDoS are not just harmful for the personal autonomy and entrepreneurial activity of the proprietor of the targeted website but they also infringe on his right to free speech and on the users right to online access; as such DDoS could not qualify as free speech. In this case, contrary to the civil rights movement, it is not the right to property that trumps the right to free speech; it is the positive obligation of the state to guarantee the right to free speech for everyone.

6. CONCLUDING REMARKS

It is true that there are certain noticeable similarities between DDoS and acts of civil disobedience. The fact that these assaults largely rely on massive participation (at least in principle), while at the same time they seem to be disseminating a message through disruption has given rise to the metaphor of DDoS as «digital sit-ins». Analogies however always carry the risk of oversimplification. The paper has attempted to demonstrate that accepting this metaphor would have actually been an unjustified generalization, which would hopefully been refuted in courts.

---

63 It is also worth recalling that this conclusion was reached based on the assumption that a website cannot be considered a public forum.

64 A Freed, DDOS Attacks Aim to Censor Human Rights Groups, available online at http://www.infosecisland.com/blogview/9322-DDOS-Attacks-Aim-to-Censor-Human-Rights-Groups.html, accessed 3/5/2012; https://www.eff.org/deeplinks/2012/03/week-censorship-denmark-tajikistan-uzbekistan, accessed 3/5/2012

65 http://www.dw.de/dw/article/0,,15155182,00.html, accessed 3/5/2012

On balance the overall picture seems to be that DDoS cannot to be considered as the digital parallel to the occurrence of sit-ins in offline reality: The fact that DDoS are proscribed acts of particularly aggressive nature combined to the threats incurred for free speech online would undercut the feasibility of granting them free speech protection. As a final remark, it should be noted that instead of resorting to misleading metaphors, it is essential to articulate a robust conceptual framework regarding DDoS and other acts of 'hacktivism', which deserves more attention than this paper has been able to give it. To do otherwise would risk the danger of criminalizing the tools and net architectural principles exploited to facilitate DDoS attacks.

7. BIBLIOGRAPHY

Atton, Ch. 2004. An Alternative Internet. Edinburgh Edinburgh University Press.

Ayres, J. 2003. From Streets to the Internet: The Cyber Diffusion of Contention. The Annals of the American Academy of Political and Social Science 566 (1).

Blodgett B, A Tapia. When Protests Go Virtual: How Organzing Social Protests in Virtual Words Changes The Nature of Organizing Paper presented at the AMCIS 2010 Procceedings, paper 553,

Burk, D. 2000. The Trouble with Tresspass. J Small & Emerging Bus. L. 4:27.

Castells, M. 2012. Networks of Outrage and Hope: Social Movements in the Internet Age. Cambridge: Polity Press

Chandler, J. 2003-2004. Liability For Botnet Attacks. U Ottawa L. & Tech. J. 231.

Clayton, G. 2000. Reclaiming Public Ground: The Right to Peaceful Assembly. The Modern Law Rev 23 (2).

Coleman, G. 2011. Hacker Politics and Publics. Public Culture 23 (3).

Costanza-Schock, S. 2003. Mapping the Repertoire of Electronic Contention. In Representing Resistance: Media, Civil Disobedience and the Global Justice Movement, ed. D Pompper A Oppel. London: Praeger.

Denning, D. 2001. Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Networks and Netwars: The Future of Terror, Crime and Militancy, ed. D Rohnfeld J Aquila. Santa Monica: RAND Corporation.

Diani, M. 2000. Social Movement Networks: Virtual and Real. Information, Communication and Society 3 (3).

Dominguez, R. 2009. Electronic Civil Disobedience: Inventing the Future of Online Agitprop Theater PMLA Publications Of The Modern Language Association Of America 124 (5).

Doyston, B. 2012. What Exactly Does The Occupy Movement Want? The Humanist.

Sinrod E, and W Reilly. 2000. Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws. Santa Clara Computer and High Technology Law Journal 6 (2)

Zuckerman, E, H Roberts, R McGrady, J York, and J Palfrey. 2010. 2010 Report on Distributed Denial of Service (DDOS) Attacks. The Berkman Center for internet and Society at the Harvard University 16.

Edwards, L. 2004. Dawn of the Death of Distributed Denial of Service: How to Kill Zombies. Cardozo Arts and Entertainment 24.

Ensemble, Critical Art. 1996. Electronic Civil Disobedience and Other Unpopular Ideas. Brooklyn: NY.

Epstein, A. 2003. Cybertrespass. University of Chicago Law Rev 70.

Epstein, RA. 1997. Takings, Exclusivity and Speech: The Legacy of PruneYard v. Robins. The Unive of Chicago Law Rev 64 (1).

Fafinski, S. 2008. Computer Misuse: the Implications of the Police and Justice Act 2006. Journal of Criminal Law 72 (1).

Feldman, D. 1993. Civil Liberties and Human Rights in England and Wales Oxford: Clarendon.

Fenwick, H. 1999. The Right to Protest, The Human Rights Act and the Margin of Appreciation. The Modern Law Rev 62.

Fenwick, H. 2002, 3rd edition. Civil Liberties and Human Rights. London: Cavendish Pub.

Fuchs, Christian. 2012. Some Reflections on Manuel Castell's Book Networks of Outrage and Hope. tripleC 10 (2).

Garrett, R. 2006. Protest in an Information Society: A Review of Literature on Social Movements and New ICTs. Information, Communication and Society 9 (2).

Gladwell, M, and Clay Shirky. 2011. From Innovation to Revolution: Do Social Media Make Protests Possible? Social Affairs 90 (2).

Gora, J, D Goldberger, G Stern, and M Halperin. 1991. The right to Protest: The Basic ACLU Giode to Free Expression. Carbondale: Ilinois University Press.

Grimmelman, J. 2010. The Internet is a Semi-Commons. Fordham L. Rev. 78.

Roberts H, E Zuckerman, R Faris, J York, and J Palfrey. 2011. The Evolving Landscape of Internet Control: A Summary of Our Recent Research and Recommendations. The Berkman Center for Internet and Society at Harvard University 5.

Clark J, and N Themudo. 2003. The Age of Protest: Internet-based 'dot causes' and the 'anti-globalization' Movement. In Globalizing Civic Engagement, Civil Society and Transnational Action, ed. J Clark. London: Earthscan Pub Ltd.

Mirkovic J, and P Reiher. 2004. A Taxonomy of DDOS Attack and DDOS Defence Mechanisms. ACM SIGCOM Computer Communications Review 34 (2).

Van Laer J, and P Van Aelst. 2010. Internet and Social Movement Action Repertoires. Information, Communication and Society.

McCarthy JD, and C McPhail. 2006. Places of Protest: The Public Forum in Principle and Practise. Mobilization: An International Quarterly 11 (2).

Kalven, H. 1965. The Concept of Public Forum: Cox v. Louisiana. Sup. Ct. Rev.

Klang, M. 2004a. Civil Disobedience Online. Journal of Information, Communication & Ethics in Society 2 (2).

Klang, M. 2004b. Virtual Sit-ins, Civil Disobedience and Cyberterrorism In Human Rights in the Digital Age, eds. M Klang, and A Murray. London: Cavendish Publishing.

Kreimer, S. 2001. Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet. U. Pa. L. Rev. 150.

Lane, J. 2003. The Digital Zapatistas. The Drama Review 47 (2).

Mcaughey M, and M Ayers. 2003. Cyberactivism: Online Activism in Theory and Practice. New York: Routledge.

Marion, and Goodrum. 2000. Terrorism of Civil Disobedience: Toward a Hacktivist Ethic Computers and Society.

McLaurin, J. 2011. Making Cyberspace Safe for Democracy:The Challenge Posed by Denial-of-Service Attacks. Yale Law & Policy Rev 30.

Meikle, G. 2002. Future Active: Media Activism and the Internet. New York: Routledge.

Mitchell, D. 2003. The Liberalization of Free Speech: Or How Protest in Public Space is Silenced Stanford Agora: An Online Journal of Legal Perspectives

Morozov, E. 2010. The Net Delusion: How Not to Liberate the World. London: Allen Lane.

Morozov, E. 2011. The Net Delusion: The Dark Side of Internet Freedom. PublicAffairs.

Nimmer, M. 1973. The Meaning of Symbolic Speech Under the First Amendment. UCLA L Rev 21.

Post, R. 1987. Between Governance Management: The History and Theory of the Public Forum. UCLA L Rev 34.

Psimitis, M 2011, 'Collective Identities Versus Social Exclusion: The December 2008 Greek Youth Movement', The Greek Review of Social Research, vol. Special issue 136 C

Sakellaropoulos, S 2012, 'On the Causes and Significance of the December 2008 Social Explosion in Greece', Science & Society, Vol. 76, No. 3, July 2012, 340–, vol. 76

Sotiris, P 2010, 'Rebels with a Cause: The December 2008 Greek Youth Movement as the Condensation of Deeper Social and Political Contradictions', International Journal of Urban and Regional Research, vol. 34, no. 1

Taylor R, and R Phillips. 1831. Intelligence and Miscellaneous Articles. The Philosophical Magazine: Or Annals of Chemistry, Mathematics, Astronomy, Natural History and General Science IX.

Rachman, R. 2012. The Legal Measure Against Denial of Service (DoS) Attacks Adopted by the United Kingdom Legislature: Should Malaysia Follow Suit? Int J Law Info Tech 20 (2).

Rawls, J. 1971. Theory of Justice. Harvard University Press.

Rawls, J. 1996. Civil Disodedience and the Social Contract. In Morality and Moral Controversies, ed. J Arthur. Prentice Hall College Div.

Reynolds, W. 2002. The Legal History of the Great Sit-in Case of Bell v. Maryland. Maryland Law Rev 6111.

Rheingold, H. 1993. The Virtual Community: Homesteading on the Electronic Frontier. Readin MA: Addison-Wesley.

Samuel, A. 2004. Hackticism and the Future of Political Participation. Cambridge MA: Harvard University Press.

Shepard, H. 2012. Labor and Occupy Wall Street: Common Causes and Uneasy Alliances. The Journal of Labor and Society 15.

Tilly, Ch. 1984. Social Movements and National Politics. In Statemaking and Social Movements: Essays in History and Theory, eds. C Bright, and S Harding. Ann Arbor MI: University of Michigan Press.

W Van De Donk, B Loader, P Nixon, and D Rucht. 2004. Cyber Protest: New Media, CItizens and Social Movements London: Routledge.

Wray, S. 1998. On Electronic Civil Disobedience. Peace Review 11 (1).

Yar, M. 2006. Cybercrime and Society. London: Thousand Oaks: Sage Publications Ltd.

COMUNICACIONES SOBRE ADMINISTRACIÓN ELECTRÓNICA

IMPULSO DE LA FACTURA ELECTRÓNICA EN EL SECTOR PÚBLICO

Ana María Delgado García
Catedrática de Derecho Financiero y Tributario
Universitat Oberta de Catalunya

RESUMEN: La Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica y Creación del Registro Contable de Facturas en el Sector Público, ha introducido algunas novedades en la normativa sobre el uso de la factura electrónica en las administraciones públicas. Mediante esta norma se pretende fundamentalmente luchar contra la morosidad de las administraciones públicas, a través del impulso de la utilización de la factura electrónica y la creación de un registro contable, de forma que se agilicen los procedimientos de pago a los proveedores y se conozcan con más detalle las facturas pendientes de pago.

En esta norma legal también se regulan, entre otros temas, el registro contable de facturas y el procedimiento de tramitación en las administraciones públicas, los efectos de la recepción de la factura electrónica, las facultades de los órganos de control y colaboración con la Agencia Estatal de Administración Tributaria, la validez de la factura electrónica ante las administraciones públicas y sus efectos tributarios, el intercambio de información entre la hacienda pública y los órganos pagadores de las administraciones públicas sobre los deudores de estas y los pagos a los proveedores, la factura electrónica en las empresas que presten servicios al público en general de especial trascendencia económica y la eficacia ejecutiva de la factura electrónica.

PALABRAS CLAVE: Factura electrónica, sector público, administración electrónica, impuestos, morosidad.

1. LA FACTURACIÓN ELECTRÓNICA EN EL SECTOR PRIVADO

Antes de analizar la legislación sobre la factura electrónica en el sector público, es conveniente efectuar un breve repaso de la normativa actual sobre la facturación electrónica en el sector privado, pues, aunque el principal objetivo, como veremos a continuación, de la Ley 25/2013, de 27 de diciembre, es el impulso de la factura electrónica en el sector público, también afecta esta regulación al fomento de la utilización de la factura electrónica en el sector privado.

La factura constituye, sin duda alguna, una de las herramientas de información con que cuenta la administración tributaria para ejercer un control efectivo sobre el cumplimiento de los deberes tributarios y, al mismo tiempo, la factura se configura también

como requisito para aplicar determinados gastos y deducciones y para el ejercicio de los derechos de repercusión y deducción del impuesto sobre el valor añadido (IVA).[1]

La facturación electrónica contribuye a una aplicación de los tributos más rápida y eficaz, al tiempo que ayuda a disminuir la presión fiscal indirecta de los obligados tributarios.[2]

Por otro lado, no hay que olvidar que la factura, como documento en el que se plasma el objeto de un contrato, es configurada por la normativa mercantil y fiscal como uno de los elementos documentales del contrato más importantes.

La obligación de facturar que incumbe a los empresarios y profesionales está contemplada, con carácter general, en el art. 29.2.e de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT). Además, dispone el art. 164.1.3º de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido (LIVA) que los sujetos pasivos del impuesto estarán obligados, con los requisitos, límites y condiciones que se determinen reglamentariamente, a expedir y entregar factura de todas sus operaciones.

Asimismo, el art. 88.2 LIVA, cuando regula la repercusión del impuesto, establece que la misma deberá efectuarse mediante factura o documento sustitutivo, en las condiciones y con los requisitos que se determinen reglamentariamente. Tales preceptos están desarrollados por lo previsto en los arts. 62 a 70 del Real Decreto 1624/1992, de 29 de diciembre, por el que se aprueba el Reglamento del Impuesto sobre el Valor Añadido (RIVA), y en el Real Decreto 1619/2012, de 30 de noviembre, que aprueba el Reglamento por el que se regulan las Obligaciones de Facturación (ROF).

Las facturas expedidas por el empresario o profesional, por su cliente o por un tercero, en nombre y por cuenta del citado empresario o profesional, podrán ser transmitidas por medios electrónicos, siempre que, en este último caso, el destinatario de las facturas haya dado su consentimiento y los medios electrónicos utilizados en su transmisión garanticen la autenticidad de su origen y la integridad de su contenido (art. 164.2 LIVA).[3]

Por otro lado, el art. 165.1 LIVA preceptúa que las facturas recibidas, los justificantes contables, las facturas expedidas y las copias de las demás facturas expedidas deberán conservarse, incluso por medios electrónicos, durante el plazo de prescripción del im-

---

1 Véase al respecto OLIVER CUELLO, Rafael: Internet y tributos, Bosch, Barcelona, 2012, págs. 308-319.

2 Sobre esta materia véase MARTOS GARCÍA, Juan Jesús: «La integridad del contenido y la autenticidad de origen en la transmisión o puesta a disposición de la factura», *Revista Internet, Derecho y Política*, nº 12, 2011, págs. 85-94.

3 Véase sobre este tema DELGADO GARCÍA, Ana María: «Los medios electrónicos y las obligaciones formales en el ámbito tributario», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 28, 2012, págs. 19-40.

puesto. Asimismo, cuando el sujeto pasivo conserve por medios electrónicos las facturas expedidas o recibidas se deberá garantizar a la administración tributaria tanto el acceso en línea a dichas facturas como su carga remota y utilización. La anterior obligación será independiente del lugar de conservación (art. 165.3 LIVA).

Por factura electrónica debe entenderse, de conformidad con lo dispuesto en el art. 1 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor. A su vez, conforme a lo dispuesto por el art. 3.5 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, en su redacción dada por la Ley 56/2007, de 28 de diciembre, se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.[4]

El ROF recoge las modificaciones introducidas en esta materia por la Directiva 2010/45/UE del Consejo, de 13 de julio. Entra en vigor el 1 de enero de 2013 y deroga el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1496/2003, de 28 de noviembre.

En cuanto a las novedades introducidas por el RD 1619/2012, de 30 de noviembre, según su preámbulo, para una mayor seguridad jurídica de los empresarios o profesionales, se aclaran los casos en los que se deben aplicar las normas de facturación establecidas en dicho ROF. Como novedad relativa a la obligación de expedir factura, se establece que no se exigirá tal obligación en el caso de determinadas prestaciones de servicios financieros y de seguros, salvo cuando dichas operaciones se entiendan realizadas en el territorio de aplicación del impuesto, o en otro Estado miembro de la UE, y estén sujetas y no exentas.

Con la finalidad de establecer un sistema armonizado de facturación en el ámbito de la Unión Europea y de promover y facilitar el funcionamiento de los pequeños y medianos empresarios así como de los profesionales, se establece un sistema de facturación basado en dos tipos de facturas: la factura completa u ordinaria y la factura simplificada, que viene a sustituir a los denominados tiques.

---

4 En relación con la naturaleza de la factura electrónica, hay que tener presente que la misma es una factura original y, por consiguiente, no constituye un documento sustitutivo de la factura, ya que no se trata de un documento que no vaya a permitir ejercitar el derecho a la deducción en cuota o sobre la base de sus destinatarios ni nos encontramos ante un documento equivalente a la factura (que, a diferencia del documento sustitutivo, y pese a no reunir los requisitos de una factura, surte sus mismos efectos). Tampoco se trata de un duplicado del original de la factura (como en el caso de la operación en la que concurran varios destinatarios o en el de pérdida del original por cualquier causa) ni de una copia del original de la factura.

Las facturas simplificadas tienen un contenido más reducido que las facturas completas u ordinarias y, salvo algunas excepciones, podrán expedirse, a elección del obligado a su expedición: cuando su importe no exceda de 400 euros, IVA incluido; cuando se trate de facturas rectificativas; o bien cuando su importe no exceda de 3.000 euros, IVA incluido, y se trate, en este último caso, de alguno de los supuestos respecto de los que tradicionalmente se ha autorizado la expedición de tiques en sustitución de facturas.

Asimismo, según el preámbulo del RD 1619/2012, la nueva regulación comunitaria en materia de facturación supone un decidido impulso a la facturación electrónica, bajo el principio de un mismo trato para la factura en papel y la factura electrónica, como instrumento para reducir costes y hacer más competitivas a las empresas. Se establece, en este sentido, una nueva definición de factura electrónica como aquella factura que, cumpliendo los requisitos establecidos en el propio Reglamento, haya sido expedida y recibida en formato electrónico.

En todo caso, las facturas en papel o electrónicas deben reflejar la realidad de las operaciones que documentan y corresponderá a los sujetos pasivos garantizar esta certidumbre durante toda su vigencia, sin que esta exigencia pueda suponer la imposición de nuevas cargas administrativas a los empresarios o profesionales. De esta forma, el sujeto pasivo podrá garantizar la autenticidad, integridad y legibilidad de las facturas que expida o conserve mediante los controles de gestión o de auditoría usuales de su actividad empresarial o profesional.

Esta igualdad de trato entre la factura en papel y la electrónica amplía, por tanto, las posibilidades para que el sujeto pasivo pueda expedir facturas por vía electrónica sin necesidad de que la misma quede sujeta al empleo de una tecnología determinada. No obstante, para garantizar la seguridad jurídica de los sujetos pasivos que ya venían utilizando el intercambio electrónico de datos (EDI) y la firma electrónica avanzada, este Reglamento reconoce expresamente que dichas tecnologías, que dejan de ser obligatorias, garantizan la autenticidad del origen y la integridad del contenido de las facturas electrónicas.

Los sujetos pasivos, asimismo, podrán seguir comunicando a la Agencia Estatal de Administración Tributaria, con carácter previo a su utilización, los medios que consideren que garantizan las condiciones citadas, al objeto de que sean, en su caso, validados por la misma.

Finalmente, para mejorar el funcionamiento del mercado interior, se impone un plazo armonizado para la expedición de las facturas correspondientes a determinadas entregas de bienes o prestaciones de servicios intracomunitarias. Asimismo, con la finalidad de facilitar la gestión administrativa de los sujetos pasivos, se ha estimado conveniente aplicar ese mismo plazo armonizado a todas las operaciones efectuadas para otros empresarios o profesionales, tanto interiores como transfronterizas. Este plazo afecta, igualmente, a las facturas recapitulativas.

En relación con los medios de expedición de las facturas, concretamente, el art. 8.1 ROF dispone que «las facturas podrán expedirse por cualquier medio, en papel o en

formato electrónico, que permita garantizar al obligado a su expedición la autenticidad de su origen, la integridad de su contenido y su legibilidad, desde su fecha de expedición y durante todo el periodo de conservación». La autenticidad del origen de la factura, en papel o electrónica, garantizará la identidad del obligado a su expedición y del emisor de la factura. La integridad del contenido de la factura, en papel o electrónica, garantizará que el mismo no ha sido modificado (art. 8.2 ROF).

La autenticidad del origen y la integridad del contenido de la factura, en papel o electrónica, podrán garantizarse por cualquier medio de prueba admitido en Derecho, según establece el art. 8.3 ROF. En particular, la autenticidad del origen y la integridad del contenido de la factura podrán garantizarse mediante los controles de gestión usuales de la actividad empresarial o profesional del sujeto pasivo. Los referidos controles de gestión deberán permitir crear una pista de auditoría fiable que establezca la necesaria conexión entre la factura y la entrega de bienes o prestación de servicios que la misma documenta.

En cuanto al concepto de factura electrónica, el art. 9.1 ROF dispone que «se entenderá por factura electrónica aquella factura que se ajuste a lo establecido en este Reglamento y que haya sido expedida y recibida en formato electrónico». La expedición de la factura electrónica, según aclara el art. 9.2 ROF, estará condicionada a que su destinatario haya dado su consentimiento. Respecto a la autenticidad del origen y la integridad del contenido de la factura electrónica, según el art. 10.1 ROF, podrán garantizarse por cualquiera de los medios señalados en el art. 8 ROF a los que ya se ha aludido.

En particular, la autenticidad del origen y la integridad del contenido de la factura electrónica quedarán garantizadas por alguna de las siguientes formas: a) mediante una firma electrónica avanzada de acuerdo con lo dispuesto en el artículo 2.2 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, basada, bien en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas, de acuerdo con lo dispuesto en los apartados 6 y 10 del art. 2 de la mencionada Directiva, o bien, en un certificado reconocido, de acuerdo con lo dispuesto en el apartado 10 del art. 2 de la mencionada Directiva; b) mediante un intercambio electrónico de datos (EDI), tal como se define en el art. 2 del anexo I de la Recomendación 94/820/CE de la Comisión, de 19 de octubre de 1994, relativa a los aspectos jurídicos del intercambio electrónico de datos, cuando el acuerdo relativo a este intercambio prevea la utilización de procedimientos que garanticen la autenticidad del origen y la integridad de los datos; c) mediante otros medios que los interesados hayan comunicado a la AEAT con carácter previo a su utilización y hayan sido validados por la misma.

Por último, en el caso de lotes que incluyan varias facturas electrónicas remitidas simultáneamente al mismo destinatario, según el art. 10.2 ROF, los detalles comunes a las distintas facturas podrán mencionarse una sola vez, siempre que se tenga acceso para cada factura a la totalidad de la información.

2. LA LEY 25/2013, DE 27 DE DICIEMBRE, DE IMPULSO DE LA FACTURA ELECTRÓNICA EN EL SECTOR PÚBLICO

Una vez efectuado este breve repaso introductorio sobre la regulación de la facturación electrónica en el sector privado, a continuación se analiza la reciente legislación sobre la factura electrónica en el sector público. En este sentido, el objeto de la Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica y Creación del Registro Contable de Facturas en el Sector Público, de acuerdo con su art. 1, es impulsar el uso de la factura electrónica, crear el registro contable de facturas, regular el procedimiento para su tramitación en las administraciones públicas y las actuaciones de seguimiento por los órganos competentes.

Según indica su preámbulo, la Ley 25/2013 establece una serie de reformas estructurales que impulsarán el uso de la factura electrónica, creando el registro contable, lo que permitirá agilizar los procedimientos de pago al proveedor y dar certeza de las facturas pendientes de pago existentes.

En dicho preámbulo de la Ley 25/2013 se afirma, asimismo, que «este control informatizado y sistematizado de las facturas favorecerá un seguimiento riguroso de la morosidad a través de un indicador, el periodo medio de pagos, que visualizará el volumen de deuda comercial de las administraciones y permitirá, llegado el caso, aplicar los nuevos mecanismos previstos por la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, en la que el control de la deuda comercial forma parte del principio de sostenibilidad financiera».

Por lo tanto, según la justificación de la citada norma legal en su preámbulo, «para fortalecer esta necesaria protección del proveedor se facilita su relación con las administraciones públicas favoreciendo el uso de la factura electrónica y su gestión y tramitación telemática (…). Asimismo, esta protección se verá reforzada con un mejor control contable de las facturas recibidas por las administraciones, lo cual permitirá no solo hacer un mejor seguimiento del cumplimiento de los compromisos de pago de las administraciones públicas, sino también, un mejor control del gasto público y del déficit, lo que generará una mayor confianza en las cuentas públicas».

A nuestro juicio, es evidente que la Ley 25/2013 tiene como principal objetivo impulsar la factura electrónica, sobre todo en el sector público, aunque también en el privado. Ahora bien, tal vez la aportación más importante de esta norma no sea tanto este necesario fomento de la facturación electrónica, sino más bien la introducción de toda una nueva y detallada normativa sobre el registro contable de facturas en el sector público.

En efecto, en nuestra opinión, quizá más relevante que la obligación, vigente a partir del 15 enero de 2015, de presentación de la factura electrónica, son las previsiones de la Ley por la que se crea el registro contable de facturas del sector público y se regula un nuevo procedimiento para su tramitación, que introduce la obligación de su remisión a este registro contable antes que al órgano gestor.

Este nuevo procedimiento de gestión de facturas supone, a nuestro juicio, una novedad muy importante, ya que hasta el momento las facturas se presentaban ante el órgano gestor sin conocimiento previo del órgano contable, que no tenía constancia de su presentación hasta que se tramitaba el procedimiento de pago. En este sentido, consideramos que la obligación de constancia registral debería reforzar la protección del proveedor y evitar las facturas pendientes de pago en poder de los órganos administrativos.

Por ello, a nuestro entender, el nuevo procedimiento de facturación debería permitir un mejor seguimiento y control de los pagos a proveedores, tanto para velar por el pago de las facturas pendientes, como para conocer los periodos medios de pago de la administración correspondiente, a los efectos de la aplicación, en su caso, de las previsiones contenidas en la Ley Orgánica 9/2013, de 20 de diciembre, de Control de la Deuda Comercial en el Sector Público. La Ley 25/2013 atribuye, además, como veremos más adelante, funciones de control y de información sobre la tramitación de las facturas a los órganos contables y de intervención.

En cuanto al ámbito de aplicación, esta Ley 25/2013, de acuerdo con lo dispuesto en el art. 2, se aplica a las facturas emitidas en el marco de las relaciones jurídicas entre proveedores de bienes y servicios y las administraciones públicas (entendiendo por tales los entes, organismos y entidades a que se refiere el art. 3.2 del Real Decreto Legislativo 3/2011, de 14 de noviembre, que aprueba el Texto Refundido de la Ley de Contratos del Sector Público, así como las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social).

Respecto a la entrada en vigor de la Ley 25/2013, conviene tener en cuenta que, de acuerdo con la DF 8ª, la norma entra en vigor a los veinte días de su publicación en el Boletín Oficial del Estado, es decir, el 17 de enero de 2014.

No obstante, el art. 4, sobre obligaciones de presentación de factura electrónica, entra en vigor el 15 de enero de 2015. Al igual que la Disposición Final Segunda, sobre la facturación electrónica en las empresas que prestan servicios de especial trascendencia económica. Y el art. 9, sobre anotación en el registro contable de facturas, entra en vigor el 1 de enero de 2014.

3. OBLIGACIÓN DE PRESENTACIÓN DE FACTURAS ANTE LAS ADMINISTRACIONES PÚBLICAS

Según el art. 4 de la Ley 25/2013, estarán obligadas al uso de la factura electrónica las entidades siguientes: sociedades anónimas, sociedades de responsabilidad limitada, personas jurídicas y entidades sin personalidad jurídica que carezcan de nacionalidad española, establecimientos permanentes y sucursales de entidades no residentes en territorio español, uniones temporales de empresas, agrupaciones de interés económico, agrupaciones de interés económico europeas, fondos de pensiones, fondos de capital

riesgo, fondos de inversiones, fondos de utilización de activos, fondos de regularización del mercado hipotecario, fondos de titulización hipotecaria y fondos de garantía de inversiones.

No obstante, es importante tener en cuenta que las administraciones públicas podrán excluir reglamentariamente de esta obligación de facturación electrónica a las facturas cuyo importe sea de hasta 5.000 euros y a las emitidas por los proveedores a los servicios en el exterior de las administraciones públicas.

Las obligaciones previstas en este artículo no serán exigibles hasta el 15 de enero de 2015.

Tal como prevé el art. 3 de la Ley 25/2013, el proveedor que haya expedido la factura por los servicios prestados o bienes entregados a cualquier administración pública tendrá la obligación de presentarla ante un registro administrativo (en los términos previstos en el art. 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común) en el plazo de treinta días desde la fecha de entrega efectiva de las mercancías o la prestación de servicios.

4. FACTURA ELECTRÓNICA EN LAS ADMINISTRACIONES PÚBLICAS

Las facturas electrónicas que se remitan a las administraciones públicas, de acuerdo con el art. 5 de la Ley 25/2013, deberán tener un formato estructurado y estar firmadas con firma electrónica avanzada basada en un certificado reconocido, de acuerdo con lo dispuesto en el art. 10.1.a del Real Decreto 1619/2012, de 30 de noviembre, que aprueba el Reglamento por el que se regulan las Obligaciones de Facturación.

También se admitirá el sello electrónico avanzado basado en un certificado reconocido, que, según se define en la propia Ley 25/2013, es el conjunto de datos en forma electrónica, consignados o asociados con facturas electrónicas, que pueden ser utilizados por personas jurídicas y entidades sin personalidad jurídica para garantizar el origen y la integridad de su contenido.

En tanto no se desarrolle el contenido de este sello electrónico avanzado, las facturas electrónicas podrán garantizar su autenticidad e integridad mediante un certificado que resulte válido en la plataforma de validación de certificados electrónicos del Ministerio de Hacienda y Administraciones Públicas.[5]

5 Por Orden ministerial se determinará el formato estructurado de la factura electrónica. La Disposición Adicional Segunda de la Ley 25/2013 establece el formato que se aplicará a las facturas remitidas a la administración en tanto no se apruebe esta Orden.

Se establece, por otra parte, en el art. 6 de la Ley 25/2013 que el Estado, las comunidades autónomas y las entidades locales dispondrán de un punto general de entrada de facturas electrónicas a través del cual se recibirán todas las facturas electrónicas que correspondan a entidades, entes y organismos vinculados o dependientes. Ahora bien, las entidades locales podrán adherirse a la utilización del punto general de entrada de facturas electrónicas que proporcione su diputación, comunidad autónoma o el Estado. Asimismo, las comunidades autónomas podrán adherirse a la utilización del punto general de entrada de facturas electrónicas que proporcione el Estado.

Tal como dispone este precepto legal dedicado al punto general de entrada de facturas electrónicas, en su apartado 4, todas las facturas electrónicas presentadas a través del mismo producirán una entrada automática en un registro electrónico de la administración pública gestora de dicho punto general de entrada de facturas electrónicas, proporcionando un acuse de recibo electrónico con acreditación de la fecha y hora de presentación.

A este respecto, de acuerdo con las previsiones del art. 6.5 de la Ley 25/2013, el punto general de entrada de facturas electrónicas proporcionará un servicio automático de puesta a disposición o de remisión electrónica de las mismas a las oficinas contables competentes para su registro.

También hay que tener en cuenta que, según establece el art. 7.1 de la Ley 25/2013, la responsabilidad del archivo y custodia de las facturas electrónicas corresponde al órgano administrativo destinatario de la misma, sin perjuicio de que pueda optar por la utilización del correspondiente punto general de entrada de facturas electrónicas como medio de archivo y custodia de dichas facturas si se adhiere al mismo.

Asimismo, se debe subrayar que cuando el punto general de entrada de facturas electrónicas sea utilizado para archivo y custodia de las facturas electrónicas, su información no podrá ser empleada para la explotación o cesión de la información, salvo para el propio órgano administrativo al que corresponda la factura. Ello se entenderá sin perjuicio de las obligaciones que se puedan derivar de la normativa tributaria, tal como precisa el art. 7.2 de la Ley 25/2013.

5. REGISTRO CONTABLE DE FACTURAS Y PROCEDIMIENTO DE TRAMITACIÓN EN LAS ADMINISTRACIONES PÚBLICAS

Las administraciones públicas, según el art. 8 de la Ley 25/2013, tendrán que disponer de un registro contable de facturas que facilite su seguimiento, cuya gestión corresponderá al órgano o unidad administrativa que tenga atribuida la función de contabilidad.

En relación con el procedimiento de tramitación de facturas, el registro administrativo en el que se reciba la factura la remitirá inmediatamente a la oficina contable competente para la anotación en el registro contable de la factura (art. 9.1 de la Ley 25/2013).

No obstante, hay que tener presente que el Estado, las comunidades autónomas y los municipios de Madrid y Barcelona podrán excluir reglamentariamente de esta obligación de anotación en el registro contable a las facturas cuyo importe sea de hasta 5.000 euros, así como las facturas emitidas por los proveedores a los servicios en el exterior de cualquier administración pública.

Tal como prevé el art. 9.2 de la Ley 25/2013, la anotación de la factura en el registro contable de facturas dará lugar a la asignación del correspondiente código de identificación de dicha factura en el citado registro contable. En el caso de las facturas electrónicas dicho código será comunicado al punto general de entrada de facturas electrónicas.

Así, el órgano o unidad administrativa que tenga atribuida la función de contabilidad la remitirá o pondrá a disposición del órgano competente para tramitar, si procede, el procedimiento de conformidad con la entrega del bien o la prestación del servicio realizada por quien expidió la factura y proceder al resto de actuaciones relativas al expediente de reconocimiento de la obligación, incluida, en su caso, la remisión al órgano de control competente a efectos de la preceptiva intervención previa (art. 9.3 de la Ley 25/2013).

Finalmente, según el art. 9.4 de la Ley 25/2013, una vez reconocida la obligación por el órgano competente que corresponda, la tramitación contable de la propuesta u orden de pago identificará la factura o facturas que son objeto de la propuesta, mediante los correspondientes códigos de identificación asignados en el registro contable de facturas.

En relación con el procedimiento para la tramitación de facturas, resultan clarificadoras algunas orientaciones que ha proporcionado al respecto el propio Ministerio de Hacienda y Administraciones Públicas.[6] Se indica, en relación con el papel que desempeña la oficina contable, que constituye el primer receptor de la factura para su control contable y remisión al órgano gestor. La oficina contable es el órgano competente para la gestión del registro contable de facturas, a la que corresponde recibir la factura desde el registro en el que la haya presentado el proveedor, anotar los datos de la factura en el registro contable de facturas y su distribución a los órganos gestores.

En este contexto, respecto a los posibles errores que pudieran existir en las facturas, según aclara este documento, la oficina contable identifica los errores contables y el órgano gestor los demás, comunicándoselos a la empresa. Es decir, la oficina contable detecta los errores que se deduzcan de datos incorrectos o no cumplimentados en la factura. El órgano gestor deberá detectar otros errores que se refieran a la prestación del proveedor o del fondo de la operación. La comunicación al proveedor, cuando dé lugar a la devolución de la factura, se hará por el procedimiento inverso al de su presentación, es decir, a través de la oficina contable y el registro en el que la presentó el proveedor.

6 Véase el documento titulado FAQ sobre la Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica y Creación del Registro Contable de Facturas en el Sector Público, Ministerio de Hacienda y Administraciones Públicas, Madrid, 2014, págs. 7-9.

A este respecto, cabe preguntarse cómo se resuelven las posibles incidencias. Pues bien, según clarifica el documento ministerial citado, tal como sucedía hasta el momento, el procedimiento de devolución de la factura se deberá efectuar por el proceso inverso al de su presentación, es decir, a través de la oficina contable y el registro en el que presentó la factura el proveedor. El órgano gestor es el encargado de informar a la empresa, como venía siendo habitual.

Asimismo, hay que tener presente que la empresa puede saber en qué fecha se ha producido el registro contable de su factura, pues el proveedor podrá consultar la anotación en el registro contable de facturas a través del punto general de entrada de facturas electrónicas, cuando la factura sea electrónica, y a través del registro administrativo, cuando se trate de facturas en papel.

Es importante, por lo tanto, destacar que el proveedor podrá comprobar el estado de su factura en todo el proceso desde el registro hasta el pago, ya que el punto general de entrada de facturas electrónicas devolverá el último estado que haya notificado la oficina contable destinataria directa de la factura electrónica (estados actualizados por la unidad tramitadora y la oficina contable). En el caso de facturas en papel, la consulta de los estados de la factura se hará a través del registro administrativo.

Por otra parte, se establece en el art. 10 de la Ley 25/2013 que los órganos o unidades administrativas que tengan atribuida la función de contabilidad en las administraciones públicas efectuarán requerimientos periódicos de actuación respecto a las facturas pendientes de reconocimiento de obligación, que serán dirigidos a los órganos competentes. Además, elaborarán un informe trimestral con la relación de las facturas con respecto a las cuales hayan transcurrido más de tres meses desde que fueron anotadas y no se haya efectuado el reconocimiento de la obligación por los órganos competentes. Este informe será remitido dentro de los quince días siguientes a cada trimestre natural del año al órgano de control interno.

6. EFECTOS DE LA RECEPCIÓN DE LA FACTURA, FACULTADES DE LOS ÓRGANOS DE CONTROL Y COLABORACIÓN CON LA AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA

La recepción de la factura en el punto general de entrada de facturas electrónicas y su anotación en el registro contable de facturas, según el art. 11 de la Ley 25/2013, tendrá únicamente los efectos que de acuerdo con la citada Ley 30/1992, de 26 de noviembre, se deriven de su presentación en un registro administrativo.

En cuanto a las facultades y obligaciones de los órganos de control interno, dispone el art. 12 de la Ley 25/2013 que la Intervención General de la Administración del Estado y los órganos de control equivalentes en los ámbitos autonómico y local tendrán acceso a la documentación justificativa, a la información que conste en el re-

gistro contable de facturas, y a la contabilidad en cualquier momento. Anualmente, el órgano de control interno elaborará un informe en el que evaluará el cumplimiento de la normativa en materia de morosidad. En el caso de las entidades locales, este informe será elevado al pleno.

Y el art. 13 de la Ley 25/2013 establece que los registros contables de facturas remitirán a la Agencia Estatal de Administración Tributaria, por vía telemática, la información sobre las facturas recibidas para asegurar el cumplimiento de las obligaciones tributarias y de facturación cuyo control le corresponda.

7. VALIDEZ DE LA FACTURA ELECTRÓNICA, EFECTOS TRIBUTARIOS E INTERCAMBIO DE INFORMACIÓN

La factura electrónica prevista en esta Ley 25/2013 y su normativa de desarrollo, según la Disposición Adicional Tercera, será válida y tendrá los mismos efectos tributarios que la factura en soporte papel. En particular, podrá ser utilizada como justificante a efectos de permitir la deducibilidad de la operación de conformidad con la normativa de cada tributo y lo dispuesto en el art. 106 LGT (normas sobre medios y valoración de la prueba).

La Disposición Adicional Cuarta de la Ley 25/2013 establece que la Agencia Estatal de Administración Tributaria, los órganos de recaudación de la comunidades autónomas y entidades locales, la Tesorería General de la Seguridad Social y los órganos pagadores de las administraciones públicas intercambiarán la información sobre deudores de las administraciones y los pagos a los mismos con el objeto de realizar las actuaciones de embargo o compensación que procedan.

A estos efectos, la Agencia Estatal de Administración Tributaria creará y administrará la plataforma informática para el desarrollo de los intercambios de información y las actuaciones de gestión recaudatoria previstas en esta disposición.

8. FACTURA ELECTRÓNICA EN LAS EMPRESAS QUE PRESTEN SERVICIOS DE ESPECIAL TRASCENDENCIA

La Disposición Final Segunda de la Ley 25/2013 introduce un nuevo art. 2 bis en la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, en el que se establece que las empresas que presten servicios al público en general de especial trascendencia económica (reguladas en el art. 2.2 de la citada Ley 56/2007: fundamentalmente, compañías de suministro de electricidad, agua, gas, telecomunicaciones, entidades financieras, aseguradoras, grandes superficies, transportes y agencias de viaje) deberán expedir y remitir facturas electrónicas en sus relaciones con empresas y particulares que acepten recibirlas o que las hayan solicitado expresamente.

Este deber es independiente del tamaño de su plantilla o de su volumen anual de operaciones.

No obstante, las agencias de viaje, los servicios de transporte y las actividades de comercio al por menor solo están obligadas a emitir facturas electrónicas en los términos previstos en el párrafo anterior cuando la contratación se haya llevado a cabo por medios electrónicos.

Las obligaciones previstas en este artículo no serán exigibles hasta el 15 de enero de 2015.

Es importante subrayar que el Gobierno podrá ampliar el ámbito de aplicación de este artículo a empresas o entidades que no presten al público en general servicios de especial trascendencia económica en los casos en que se considere que deban tener una interlocución telemática con sus clientes o usuarios, por la naturaleza de los servicios que prestan, y emitan un número elevado de facturas.

En este sentido, las empresas prestadoras de servicios deberán facilitar acceso a los programas necesarios para que los usuarios puedan leer, copiar, descargar e imprimir la factura electrónica de forma gratuita sin tener que acudir a otras fuentes para proveerse de las aplicaciones necesarias para ello. Y deberán habilitar procedimientos sencillos y gratuitos para que los usuarios puedan revocar el consentimiento dado a la recepción de facturas electrónicas en cualquier momento.

9. EFICACIA EJECUTIVA DE LA FACTURA ELECTRÓNICA

La Disposición Final Segunda de la Ley 25/2013 también introduce un nuevo art. 2 ter en la citada Ley 56/2007, en el que se establece que la factura electrónica podrá pagarse mediante adeudo domiciliado si se incluye en la correspondiente extensión el identificador de cuenta de pago del deudor y en un anexo el documento que acredite el consentimiento del deudor a que se refiere la Ley 16/2009, de 13 de noviembre, de Servicios de Pago.

Asimismo, las facturas electrónicas llevarán aparejada ejecución si las partes así lo acuerdan expresamente. En ese caso, su carácter de título ejecutivo deberá figurar en la factura y el acuerdo firmado entre las partes por el que el deudor acepte dotar de eficacia ejecutiva a cada factura, en un anexo. En dicho acuerdo se hará referencia a la relación subyacente que haya originado la emisión de la factura.

La falta de pago de la factura que reúna estos requisitos, acreditada fehacientemente o, en su caso, mediante la oportuna declaración emitida por la entidad domiciliaria, faculta al acreedor para instar su pago mediante el ejercicio de una acción ejecutiva de las previstas en el art. 517 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

También es importante destacar que en las relaciones con consumidores y usuarios, la factura electrónica no podrá tener eficacia ejecutiva. Y que lo dispuesto en este art.

2 ter de la citada Ley 56/2007 no será aplicable al pago de las facturas que tengan por destinatarios a los órganos, organismos y entidades integrantes del sector público.

10. BIBLIOGRAFÍA

Delgado García, Ana María (2012). «Los medios electrónicos y las obligaciones formales en el ámbito tributario». *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 28).

Martos García, Juan Jesús (2011). «La integridad del contenido y la autenticidad de origen en la transmisión o puesta a disposición de la factura». *Revista Internet, Derecho y Política* (núm. 12).

Oliver Cuello, Rafael (2012). *Internet y tributos*. Barcelona: Bosch.

LA ADMINISTRACIÓN ELECTRÓNICA COMO INSTRUMENTO DE PROTECCIÓN AMBIENTAL. EN PARTICULAR, LOS SERVICIOS ELECTRÓNICOS DE INFORMACIÓN AMBIENTAL (2003-2013)

Francisco Javier Sanz Larruga
Catedrático de Derecho Administrativo
Universidad de A Coruña

RESUMEN: Se trata de exponer los instrumentos jurídicos vigentes, tanto en la Unión Europea como en España, relativos al reconocimiento del derecho de acceso a la información ambiental y la ordenación de las infraestructuras de información espacial o geográfica. En el marco de lo que se ha denominado «Derecho geo-espacial» se hace referencia a algunos de los problemas jurídicos que están planteando y plantearán en un futuro próximo el uso de las tecnologías de la información y comunicación en la política del medio ambiente. En cualquier caso, el futuro de la protección ambiental tiene en estos instrumentos de información espacial una pieza fundamental para la consecución de sus objetivos para la sostenibilidad ambiental.

PALABRAS CLAVE: Sistemas de información espacial, derecho ambiental, acceso a la información ambiental, publicidad activa ambiental.

1. INTRODUCCIÓN. EL «SISTEMA DE COMPARTIDO DE INFORMACIÓN AMBIENTAL» EN LA UNIÓN EUROPEA

Las tecnologías de la información y comunicación están aportando, desde hace varias décadas, importantes herramientas de trabajo para aplicar muchas de las medidas previstas en las políticas ambientales, tanto a nivel internacional, regional como en los Estados más avanzados. Limitándonos al ámbito de la Unión Europea debe destacarse el «sistema compartido de información medioambiental» que comprende principalmente los sistemas «Inspire» (infraestructura de información espacial en la Comunidad Europea) y «Copernicus» (programa europeo de vigilancia de la Tierra), así como otros sistemas europeos de información como el «Sistema de información sobre la biodiversidad en Europa» (BISE) y el «Sistema de Información sobre el agua para Europa» (WISE).

Estos instrumentos son poderosas herramientas para las Instituciones Comunitarias y para los Estados miembros en orden a diseñar e implementar sus normas y programas de acción en materia de medio ambiente. Pero muchos de los datos que proporcionan dichos sistemas, trascienden el ámbito de las autoridades públicas competentes en esta materia para ponerse a disposición de los ciudadanos a través de internet. Y no ya

como una mera disponibilidad graciosa de las Administraciones Públicas sino como un verdadero derecho subjetivo.

En efecto, por lo que se refiere a la Unión Europea, la aprobación –en el seno de la Comisión Económica para Europa de las Naciones Unidas– del Convenio de Aarhus, el 25 de junio de 1998, sobre acceso a la información, la participación del público en la toma de decisiones y el acceso a la justicia en materia de medio ambiente, y su recepción en el ordenamiento comunitario en virtud de la Directiva del Parlamento Europeo y del Consejo 2003/4/CE, de 28 de enero, ha significado que la puesta a disposición de información ambiental –su recogida y difusión– por las Administraciones públicas ambientales sea una obligación jurídica que puede exigirse por el derecho subjetivo de los ciudadanos (del «público», es decir, cualquier persona física o jurídica) de acceso a la misma, previa solicitud.

Entre la información que es preciso disponer para hacer posible la eficaz aplicación de las medidas ambientales (especialmente las preventivas) es muy importante la «información espacial» cada vez más implantada gracias al desarrollo de los «sistemas de información geográfica» (SIG). En la Unión Europea la elaboración de la política ambiental –tal como está formulada en los Tratados, desde que se introdujo en 1986 con el Acta Única Europea– tendrá especialmente en cuenta «los datos científicos y técnicos disponibles» (art. 191,3 del Tratado de Funcionamiento de la Unión Europea). Asimismo, los últimos Programas de Acción comunitaria en materia de medio ambiente han venido destacando la importancia de una buena información espacial que, además, se ponga en práctica de modo integrado, teniendo en cuenta las diferencias regionales y locales de la Unión Europea.

El vigente Programa General de Acción en materia de medio ambiente hasta el 2020 (el 7º) –aprobado recientemente por Decisión 1386/2013/UE bajo el título «vivir bien, respetando los límites de nuestro planeta»– contempla como su «Objetivos prioritario nº 5: mejorar la base de conocimientos e información de la política de la Unión de medio ambiente». Con tal fin se propone entre otros objetivos garantizar la consolidación del «interfaz ciencia-política, en particular en lo que se refiere a la accesibilidad de los datos para los ciudadanos…». (apartado 73, c) del VII Programa).

Centrándonos ahora en la «información espacial» para implementar la política ambiental en la Unión Europea es fundamental referirse a la Directiva 2007/2/CE del Parlamento y del Consejo de 14 de marzo de 2007, por la que se establece una infraestructura de información espacial en la Comunidad Europea –también conocida como «Directiva INSPIRE»–. Esta norma comunitaria tiene por objetivo: «fijar normas generales con vistas al establecimiento de una infraestructura de información espacial en la Comunidad Europea (Inspire), orientada a la aplicación de las políticas comunitarias de medio ambiente y de políticas o actuaciones que puedan incidir en el medio ambiente» (art. 1,1). Y se presenta como complementaria a la citada Directiva 2003/4/CE de acceso a la información ambiental (cfr. art. 2,1).

La «infraestructura de información espacial» se define como «metadatos, conjuntos de datos espaciales y los servicios de datos espaciales; los servicios y tecnologías de red; los acuerdos sobre puesta en común, acceso y utilización; y los mecanismos, procesos y procedimientos de coordinación y seguimiento establecidos, gestionados o puestos a disposición de conformidad con lo dispuesto en la presente Directiva» (art. 3,1), en donde los conceptos, las aplicaciones y sistemas informáticos son esenciales a la misma («metadatos», «interoperabilidad», «geoportal Inspire», etc.). En todo caso, tal como establece el art. 4,1,b) los datos deben de estar en «formato electrónico».

En cuanto a los «metadatos» que los Estados miembros han de crear en los plazos previstos en el art. 6 de la Directiva –en las condiciones de acceso y de calidad previstos en el art. 5,2–, aparte de los datos geográficos principales (coordenadas de referencia, cuadrículas geográficas, nombres, unidades administrativas, parcelas catastrales, etc.), han de comprender un completo conjunto de informaciones espaciales relevantes para el medio ambiente (uso del suelo, servicios de utilidad público, instalaciones productivas, demografía, zonas de riesgos, condiciones atmosféricas, hábitats y biotopos, etc.).

En el art. 11 de la Directiva Inspire se relacionan una serie de servicios de red –de localización, de visualización, de descarga, de transformación, etc.– de los «metadatos» que los Estados miembros han de garantizar que «se pongan de forma gratuita a disposición del público» (art. 14,1), si bien se prevé en el art. 13 los supuestos en que aquellos podrán poner límites a dicho acceso (que son coincidentes con los previstos en la repetida Directiva 2003/4/CE).

Como señala DÍAZ DÍAZ, «La geoinformación y los servicios espaciales comienzan a emplearse para fines que van desde la seguridad nacional al cambio climático, al conocimiento del territorio y la gestión de catástrofes naturales, a redes sociales y dispositivos también móviles de navegación por satélite, a la búsqueda de fuentes alternativas de energía y el despliegue de banda ancha» (2010).

Con motivo de la «evaluación intermedia de la Directiva Inspire», a través de una consulta pública (cuyos resultados se presentarán en 2014 para la mejora y corrección de su contenido), se manifiesta la confianza en que aquella se incorpore a los Derechos internos de los Estados miembros y en que se establezcan las estructuras y mecanismos adecuados para coordinar a través de los diferentes niveles de Administración la contribución de todos aquellos que tengan interés en sus infraestructuras de información espacial, así como en la mejora del acceso automatizado de los datos y su interoperabilidad.

2. LA INFORMACIÓN AMBIENTAL Y LA INFRAESTRUCTURA DE INFORMACIÓN GEOGRÁFICA EN ESPAÑA

En el caso de España, la transposición de la Directiva 2003/4/CE tuvo lugar mediante la aprobación de la Ley 27/2006, de 18 de julio, por la que se regula los derechos de acceso

a la información, de participación pública y de acceso a la justicia en materia de medio ambiente (cfr. los trabajos de CASADO CASADO, 2013; PIGRAU SOLÉ, 2008; y RÁZQUIN LIZARRAGA y RUÍZ DE APODACA, 2007). En cuanto al derecho de acceso a la información ambiental, a lo largo de su Título II se regula tanto lo relativo a las obligaciones generales de las autoridades públicas en materia de información ambiental, entre las que se señala la de «fomentar el uso de las tecnologías de la información y de las telecomunicaciones para facilitar el acceso a la información» (art. 5,1,e), así como las «obligaciones específicas en materia de difusión ambiental» en las que destaca la exigencia sobre el uso de las tecnologías de la información y comunicación; en efecto, según dispone el art. 6:

> «2. Las autoridades públicas organizarán y actualizarán la información ambiental relevante para sus funciones que obre en su poder o en el de otra entidad en su nombre con vistas a su difusión activa y sistemática al público, *particularmente por medio de las tecnologías de la información y las telecomunicaciones siempre que pueda disponerse de las mismas*.
>
> 3. Las autoridades públicas adoptarán las medidas necesarias para garantizar que la información ambiental *se haga disponible paulatinamente en bases de datos electrónicas de fácil acceso al público a través de redes públicas de telecomunicaciones*.
>
> 4. Las *obligaciones relativas a la difusión de la información ambiental por medio de las tecnologías de la información y de las telecomunicaciones se entenderán cumplidas creando enlaces con direcciones electrónicas a través de las cuales pueda accederse a dicha información*».

Por lo que se refiere al derecho de «acceso a la información ambiental previa solicitud» –regulada en los arts. 10 y ss– también se pone de manifiesto la buena predisposición del legislador a promover los medios electrónicos y telemáticos como cuando, en relación con la «forma o formatos de la información» el art. 11,2 establece que «las autoridades públicas procurarán conservar la información ambiental que obre en su poder, o en el de otros sujetos en su nombre, en formas y formatos de fácil reproducción y acceso *mediante telecomunicaciones informáticas y por otros medios electrónicos*».

Otras referencias de interés, a los efectos de nuestra comunicación, en la Ley 27/2006, son las relativas a la previsión de un Convenio de colaboración entre la Administración General del estado y las organizaciones empresariales para la constitución de puntos de información digitalizados (cfr. Disposición Adicional 7ª) o la previsión sobre la inclusión en los registros telemáticos de la Administración General del Estado el procedimiento telemático sobre la resolución de solicitudes de información ambiental (cfr. Disposición Adicional 9ª).

Poco tiempo después de la aprobación de la Ley 27/2006, se publicó la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, lo cual vendría a consolidar y ampliar las posibilidades de las relaciones electrónicas entre las Administraciones Públicas y los ciudadanos más allá de las cuestiones relativas al medio ambiente y a establecer verdaderos derechos subjetivos «electrónicos» de los ciudadanos (cfr. en particular su art. 6º) (sobre esta Ley vid. por todos los comentarios coordinados por GAMERO CASADO y VALERO TORRIJOS, 2010, 3ª edición).

Más recientemente, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, profundiza en las exigencias de apertura informativa de las Administraciones Públicas (cfr. el estudio coordinado por GUICHOT, 2014). En su Preámbulo se refiere, como precedente de reconocimiento de acceso a la información pública, a la Ley 27/2006. En lo relativo a la «transparencia de la actividad pública» –desarrollada a lo largo de su Título I–, además de determinar el ámbito subjetivo de aplicación (el art. 2º sobre las Administraciones Públicos, organismos y entidades públicas y privadas que están obligadas a suministrar información), la Ley distingue dos modalidades de transparencia:

1ª. la llamada «publicidad activa» a la que están obligados a proporcionar los sujetos obligados en el art. 2,1 mediante su publicación «de forma periódica y actualizada» «cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública» (art. 5,1), estableciendo además que:

> «La información sujeta a las obligaciones de transparencia *será publicada en las correspondientes sedes electrónicas o páginas web* y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización» (art. 5,4).

La información que está sometida a esta obligación de «publicidad activa» se refiere tanto a la información de carácter «institucional, organizativa y de planificación» (art. 6), como de «relevancia jurídica» (art. 7º) así como la de naturaleza «económica, presupuestaria y estadística» (art. 8º). Así, por ejemplo, un tipo de información de relevancia jurídica es la relativa a los documentos que deben ser sometidos a un periodo de información pública, como los previstos en la Ley 9/2006, de 28 de abril, sobre evaluación de los efectos de determinados planes y programas en el medio ambiente.

Sobre los «principios técnicos» que han de orientar el «portal de transparencia» (previsto en el art. 10), el art. 11 exige que la información publicada se adecúe a los siguientes principios:

«a) Accesibilidad: se proporcionará información estructurada sobre los documentos y recursos de información con vistas a facilitar la identificación y búsqueda de la información.

b) Interoperabilidad: la información publicada será conforme al Esquema Nacional de Interoperabilidad, aprobado por el Real Decreto 4/2010, de 8 enero, así como a las normas técnicas de interoperabilidad.

c) Reutilización: se fomentará que la información sea publicada en formatos que permita su reutilización, de acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público y en

su normativa de desarrollo». Sobre esta cuestión es destacable la publicación coordinada por CERRILLO y GALÁN GALÁN (2008).

2ª. el «derecho de acceso a la información pública» –definiéndose ésta como «los contenidos o documentos, cualquier que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones» (art. 13)– se regular en los arts. 12 a 24 de la Ley 19/2013. Sobre el régimen jurídico para el ejercicio de dicho derecho sólo destacamos aquí la previsión de algunos límites al derecho de acceso como, por ejemplo, cuando acceder a la información suponga un perjuicio para «la protección del medio ambiente» (cfr. art. 14,1,l), si bien la aplicación de cualquier límite «será justificada y proporcionada a su objeto y finalidad de protección y atenderá a la circunstancias del caso concreto» (art. 14,2). Sobre la confidencialidad de los datos empresariales en poder de las Administraciones públicas en materia de medio ambiente cabe destacar el reciente trabajo de RAZQUIN LIZARRAGA (2013).

Una vez expuestos de forma somera los elementos del grupo normativo de la información ambiental y de la Administración electrónica en España, corresponde analizar la principal norma de transposición de la ya referida Directiva 2007/2/CE (Directiva Inspire). Directiva que fue objeto de transposición por medio de la Ley 14/2010, de 5 de julio, sobre las infraestructuras y los servicios de información geográfica en España. El objeto de esta Ley es según su art. 1,1:

> «complementar la organización de los servicios de información geográfica y fijar, de conformidad con las competencias estatales, las normas generales para el establecimiento de infraestructuras de información geográfica en España orientadas a facilitar la aplicación de políticas basadas en la información geográfica por las Administraciones Públicas y el acceso y utilización de este tipo de información, especialmente las políticas de medio ambiente y políticas o actuaciones que puedan incidir en él».

La «infraestructura de información geográfica» –«constituida por el conjunto de infraestructuras y servicios interoperables de información geográfica disponible sobre el territorio nacional, el mar territorial, la zona contigua, la plataforma continental y la zona económica exclusiva, generada bajo responsabilidad de las Administraciones Públicas» (1,2).– se define en su art. 3,1,a) como:

> «aquella estructura virtual en red integrada por datos georreferenciados y servicios interoperables de información geográfica distribuidos en diferentes sistemas de información, accesible vía Internet con un mínimo de protocolos y especificaciones normalizadas que, además de los datos, sus descripciones mediante metadatos y los servicios interoperables de información geográfica, incluya las tecnologías de búsqueda y acceso a dichos datos; las normas para su producción, gestión y difusión; los acuerdos sobre su puesta en común, acceso y utilización entre sus productores y entre éstos y los usuarios; y los mecanismos, procesos y procedimientos de coordinación y seguimiento establecidos y gestionados de conformidad con lo dispuesto en la presente ley».

La coordinación y dirección de la infraestructura de información geográfica en España se atribuye al «Consejo Superior Geográfico», sin perjuicio de las competencias sectoriales o territoriales de cada autoridad responsable (cfr. art. 4,1). Los datos geográficos y los servicios interoperables de información geográfica proporcionados a través de la Red Internet por las diferentes Administraciones y Organismos del sector público integrados en dicha Infraestructura «estarán disponibles a través del *Geoportal* de la Infraestructura de Datos Espaciales de España» (art. 5). En la Ley 14/2010 se establecen una serie de normas que deben cumplir los servicios de información geográfica (cfr. arts. 6 y 7) y, entre éstos, las «normas para asegurar la interoperabilidad» entre los sistemas de información geográfica, remitiéndose a los criterios y recomendaciones establecidos por el «Esquema nacional de Interoperabilidad» y en el «Esquema nacional de Seguridad» (cfr. art. 7,1). Sobre la importancia de la interoperabilidad de la geoinformación puede consultarse el trabajo de DÍAZ DÍAZ (2012) se desarrolla su dimensión jurídica, relativa a la relación e interacción entre los agentes jurídicos y operadores técnicos implicados en actuaciones, procesos y procedimientos administrativos, judiciales o extrajudiciales que, con soporte en sistemas de información interpretable de forma automática y reutilizable por aplicaciones, comparten datos y servicios integrados, accesibles, fiables y sostenibles en el tiempo, e intercambian conocimientos para el objeto específico requerido por su actividad.

El Capítulo III de la citada Ley 14/2010 regula los requisitos para la puesta en común de los datos geográficos y los servicios interoperables de información geográfica, así como las condiciones de acceso –generalmente gratuita– a los mismos (cfr. arts. 8 a 14). Aunque «el acceso a los servicios de información será público», también se establece la protección de «los intereses de terceros más dignos de protección y garantizándose el cumplimiento de la legislación vigente en materia de acceso a la información pública» (art. 13,1). Para el caso del acceso a la información ambiental se remite al art. 13,2 de la Ley 27/2006 –sobre las excepciones a la obligación de facilitar información ambiental– (cfr. art. 13,3,h). Así, por ejemplo, conforme a lo que establece la Orden AAA/1601/2012, de 26 de junio, por la que se dictan instrucciones sobre la aplicación en el Ministerio de Agricultura, Alimentación y Medio Ambiente, de la Ley 27/2006, una de las excepciones a la obligación de facilitar información ambiental –la relativa a la revelación de la información ambiental que pueda afectar negativamente a la protección del medio ambiente– es la que se refiera a «la localización de las especies amenazadas o a la de sus lugares de reproducción»; y, en cambio, según el criterio jurisprudencial del Tribunal de Justicia de la Unión Europea, no cabe oponer dicha excepción a la información sobre «organismos modificados genéticamente» (cfr. apartado 8º del Bloque B) del Anexo).

Con anterioridad a la aprobación de la Ley 14/2010, la Comisión Permanente del Consejo Superior Geográfico había aprobado en abril de 2002 la puesta en marcha de una «infraestructura Nacional de Datos Espaciales». La importancia de esta infraestruc-

tura es vital para eliminar las barreras políticas e institucionales que impiden el desarrollo de la información geográfica, para lo cual se necesita, según ALONSO-PASTOR:

- Asegurar que los datos son comprensibles, contienen las mismas definiciones y formatos y los períodos de actualización son adecuados.
- Promover la interoperabilidad entre diferentes fuentes de datos y sistemas.
- Reducir las restricciones de uso sin perjuicio de los derechos de propiedad intelectual y otros.
- Diseminar de forma eficaz la información sobre qué fuentes de datos están disponibles.

3. ALGUNOS PROBLEMAS JURÍDICOS QUE PUEDEN DERIVARSE DE LA IMPLANTACIÓN Y ACTIVIDAD DE LOS SERVICIOS DE INFORMACIÓN GEOGRÁFICA. DE LA ADMINISTRACIÓN ELECTRÓNICA AL «GOBIERNO ABIERTO»

La tecnología geoespacial incluye –como señala DÍAZ DÍAZ (2010)– una gama amplia de aplicaciones telemáticas e informáticas, tales como sistemas de ortofotografía aérea, servicios web (WMS), sistemas de posicionamiento global (GPS), servicios basados en geolocalización (LBS), información geográfica (SIG), etc., cada vez más utilizados por los Gobiernos y las empresas como herramientas de gestión. Desde el punta de vista del derecho, la utilización de estas técnicas, servicios y aplicaciones, que suelen estar disponibles en Internet están generado nuevos problemas jurídicos que podrían encuadrarse dentro de un nuevo «Derecho Geoespacial». En esta dirección es destacable la labor docente e investigadora del «Centre for Spatial Law and Policy» dirigido por K. D. POMFRET en los Estados Unidos de América (Cfr, también su trabajo de 2009 citado en la bibliografía). En opinión de DÍAZ DÍAZ, los principios del «Derecho geoespacial» son los siguientes:

1º. «full and open sharing» que implica, tanto:
   1) la necesaria interoperabilidad, como
   2) el fácil acceso a toda la información espacial disponible

2º. «data collecting»: es decir, el intercambio de información en los niveles nacional, federal –regional– y local; y

3º. «accesibility», o lo que es lo mismo, un grado elevado de adecuación a nivel nacional

Como hemos visto en el apartado anterior, la tecnología espacial cuenta ya con un marco jurídico que tiene como bases normativas la Directiva 2007/2/CE (Inspire) y –su transposición mediante– la Ley 14/2010 sobre infraestructuras y los servicios de información geográfica en España. El mismo autor antes citado, hace una enumeración de las

cuestiones jurídicas que pueden derivarse de este nuevo grupo normativo como la determinación de los derechos de la propiedad intelectual; la responsabilidad sobre la calidad de los datos ofrecidos; la protección de los derechos de la intimidad, la privacidad, la propia imagen (cfr. por ejemplo, la exigencia de preservar estos derechos por el servicio de «Google Street View»); la responsabilidad de los operadores de datos espaciales y servicios asociados a la información geográfica; la implantación de la interoperabilidad –interna y externa- de los datos espaciales que son compartidos por las autoridades públicas y por los usuarios privados; la disponibilidad de los datos –o no– para su reutilización (sobre la uso libre de los geodatos puede consultarse el trabajo de SÁNCHEZ ORTEGA y DE LA CUEVA, 2011); la concesión de licencias para la protección de los datos y servicios espaciales no gratuitos o no generalmente accesibles; etc.

Desde un punto de vista material, los servicios de información geográfica están desempeñando una importante función en la gestión de los riesgos naturales y en otras funciones públicas vinculadas con la seguridad y defensa nacionales, y, por supuesto, con la gestión del medio ambiente.

Sobre la aplicación de las tecnologías de la información y comunicación para la gestión del medio ambiente en España cabe destacar los importantes cometidos que están prestando los servicios de la Administración electrónica en gestión hidrológica. Como sujeto obligado en la aplicación de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, las Confederaciones Hidrográficas están adaptado –como señala MARTÍNEZ GUTIÉRREZ (2009)– su actuación administrativa a la modalidad electrónica y, más concretamente, para sus labores de control de la calidad de las aguas. En efecto, a través de dos potentes sistemas informáticos: el «sistema automático de información hidrológica» (SAIH) y el «sistema automático de información de la calidad de las aguas» (SAICA) se generan automáticamente unos informes de control que, el futuro podrán sustituir a los agentes de inspección ambiental en las tareas de policía de aguas.

Dentro de las técnicas utilizadas por la Administración hidrológica está la «teledetección» que se emplea como medio de prueba en materia de aguas con la finalidad de precisar la situación de un determinado territorio en periodos temporales diferentes. Como exponen DELGADO PIQUERAS y GALLEGO CÓRCOLES (2007), la teledetección puede definirse como «el conjunto de técnicas que analizan los datos obtenidos por sensores situados en los aviones, plataformas espaciales o satélites, siendo ésta última la más conocida y que específicamente se denomina «teledetección espacial. En un sentido amplio, la teledetección consiste en el reconocimiento de, identificación y estudio de los objetos de la superficie terrestre, a partir del estudio de la energía reflejada o emitida por los mismos».

En esta campo de la gestión hidrológica la teledetección está siendo admitida como prueba en la jurisprudencia si bien, en ocasiones, se admite su validez siempre que reúnan una serie de requisitos. Así, por ejemplo, que sean debidamente interpretados por técnicos especialista en teledetección. Sin embargo, «la validez de los informes de tele-

detección no es absoluta –como dice MARTÍNEZ GUTIÉRREZ (2009)– y en relación a los mismo prevalecen otros medios de certificación como las actas de comprobación de los datos de aprovechamiento suscritas por las Administraciones hidráulicas, al ser consideradas las últimas como «actos propios que vinculan a la Administración con carácter preferente a otras pruebas indirectas como la teledetección». En este sentido, pueden consultarse las recientes sentencias del Tribunal Superior de Justicia de Castilla-La Mancha de 26 de noviembre de 2012 (JUR\2013\7006), de 19 de noviembre de 2012 (JUR\2012\406858), de 16 de noviembre de 2012 (JUR\2012\407634) y 6 de noviembre de 2012 (JUR\2012\396479) en las que, pese a reconocer la validez de la prueba de teledetección en que se basaba la sanción impuesta por la Administración Hidrográfica (Confederación Hidrográfica del Júcar, en todos los casos), se admite el recurso de sancionado basado en otros documentos disponibles sobre el aprovechamiento del agua.

Las tecnologías de la información y comunicación pueden ofrecer importantes funciones en el ámbito urbanístico –como ha estudiado GÓMEZ MANRESA (2008)– para el cumplimiento de la exigencia constitucional y comunitaria sobre una ordenación integrada y sostenible. Es evidente que la «Directiva Inspire» es muy apropiada para la aportación de datos espaciales con el fin de una mejor ordenación del territorio y de la misma actividad urbanística. Pero adviértase, en este sentido, la gran utilidad de las técnicas de teledetección y, en general, de la infraestructura de información geográfica para el control de las infracciones urbanísticas cuya pruebas son incontestables para demostrar las variaciones ilegales de los aprovechamientos urbanísticos.

Por otras parte, como ha puesto de manifiesto SÁNCHEZ JORDÁN –desde el punto de vista del Derecho Inmobiliario y Registral– «es posible detectar algunas quiebras de la necesaria seguridad jurídica en materia de información territorial, pues frente a la presunta superioridad que algunos preceptos parecen atribuir a los datos y las representaciones gráficas contenidas en el Catastro, hay normas que admiten la incorporación de un gran volumen de información territorial al Registro de la Propiedad, generando efectos que van más allá de la mera publicidad noticia», y para evitar dichas discordancias, la autora defiende que «es preciso que el legislador adopte una decisión que resuelva los casos de discrepancia entre representaciones gráficas del territorio, lo que presupone: En primer lugar, que se dé solución a los problemas de coordinación entre Registro de la Propiedad y Catastro; en segundo término, que se decida cuál es el valor jurídico de la información territorial asociada».

Quizá todavía es temprano para valorar suficientemente la importancia de las técnicas de información espacial en la protección del medio ambiente y en la prevención de la contaminación en muchos de los sectores ambientales. En cualquier caso, resulta indiscutible que el reconocimiento jurídico en España del derecho de los ciudadanos a la información ambiental (desde el 2006) y la obligación de transparencia administrativa (de publicidad activa) que se proyecta, entre otras Administraciones Públicas, a las que tienen competencias ambientales (desde 2013), va a suponer un importante avance en la

aplicación efectiva del Derecho Ambiental, impulsado además gracias al reconocimiento de acceso a los servicios de la Administración electrónica (desde 2007).

Seguramente todas estas previsiones normativas no son suficientes y será preciso un mayor compromiso por parte de las Administraciones Públicas. En este sentido, resulta de gran interés la iniciativa promovida por la Administración del Presidente OBAMA sobre «Open Government» –basada en los principios de transparencia, participación y colaboración con los ciudadanos– que aplicada sobre la Agencia más importante en la aplicación de la política ambiental norteamericana –la «Environmental Protection Agency» (EPA)– viene desarrollando desde el año 2010. En la actualidad, está disponible en internet el «Open Government Plan 2.0» de la EPA, fechado en abril de 2012. Según este plan que sigue la «Open Government Directive» de 8 de diciembre de 2009, se ha avanzado en las siguientes materias: en cuanto a la participación de la ciudadanía en temas como la gestión de las aguas urbanas o la mejora de la comunicación en el muestreo; en la ampliación de la conciencia pública y colaboración en el desarrollo de los reglamentos; también la participación de los ciudadanos en las decisiones ambientales, etc. Incluso mediante la creación de «aplicaciones»(«apps») que permiten a los ciudadanos interactuar con las Administraciones ambientales. También es muy importante el efectivo funcionamiento de la Ley de libertad de información («Freedom of Information Act», FOIA) para acceder a la información disponible en las Administraciones Públicas.

En esta línea de «gobierno abierto» un interesante ejemplo es la puesta a disposición de los ciudadanos de la Unión Europea de una serie de aplicaciones móviles («apps») en relación con la calidad del aire en las ciudades europeas, el cálculo de la «huella ecológica» de determinados productos y actividades, la localización de las áreas protegidas de interés ecológico, los niveles de ruido, etc.

Tal como se concluía en Congreso Internacional sobre «Open Government» celebrado en la Facultad de Derecho de Valencia el pasado año 2013, una de las piezas clave del «Gobierno Abierto» es la información como materia prima para su construcción y en la capacidad de la ciudadanía para la toma de decisiones. Pero como se ha puesto de manifiesto en esta comunicación, la disponibilidad de abundante información ambiental –procedente de la infraestructura de la información espacial a la que concretamente nos hemos referido– no basta si no se articula una accesible plataforma de «publicidad activa» por parte de las Administraciones Públicas competentes y organismos concernidos en la obligación de informar, y si se garantiza y proteger el derecho de acceso a la información pública ambiental. Sólo así será una realidad el Principio 10º de la *Declaración de Río de Janeiro sobre Medio Ambiente y Desarrollo* de 1992:

> «El mejor modo de tratar las cuestiones ambientales es con la participación de todos los ciudadanos interesados, en el nivel que corresponda. En el plano nacional, toda persona deberá tener acceso adecuado a la información sobre el medio ambiente de que dispongan las autoridades públicas, incluida la información sobre los materiales y las actividades que ofrecen peligro en sus comunidades, así como la oportunidad de participar en los procesos de adopción de decisiones. Los Estados deberán facilitar y fomentar la sensibilización y la participación del público

poniendo la información a disposición de todos. Deberá proporcionarse acceso efectivo a los procedimientos judiciales y administrativos, entre éstos el resarcimiento de daños y los recursos pertinentes».

4. BIBLIOGRAFÍA

Alonso-Pastor, F.: «Gestión, uso y publicación de datos de biodiversidad y patrimonio natural para gestores. Armonización y publicación de datos y metadatos conforme la Directiva INSPIRE. 1- Definición y objetivos de la Directiva INSPIRE y de la LISIGE», disponible en la dirección de internet: http://www.gbif.es/gbif/ficheros/TallerINSPIRE2013/01_INSPIREyLISIGE.pdf

Casado Casado, L.: «El acceso a la información ambiental en España: luces y sombras», en *Revista de la Facultad de Derecho PUCP*, nº 70 (2013), pp. 241-278, disponible en la dirección de internet: http://revistas.pucp.edu.pe/index.php/derechopucp/article/viewFile/6753/6870

Cerrillo, A. y Galán Galán (coordinadores): *La reutilización de la información del sector público*, Comares, Granada, 2008.

Delgado Piqueras, F. y Gallego Córcoles, I.: *Aguas subterráneas privadas, teledetección y riego*. *Un estudio jurisprudencial*, Editorial Bomarzo, Albacete, 2007.

Díaz Díaz, E.: «Interoperabilidad jurídica de la geoinformación», comunicación presentada en las *III Jornadas Ibéricas de Infraestructuras de Datos Espaciales*, Madrid, octubre de 2012, disponible en la dirección de internet: http://www.idee.es/resources/presentaciones/JIIDE12/miercoles/C18.Articulo.pdf

Díaz Díaz, E.: «Marco jurídico y administrativo de la geoinformación. Importancia jurídica de los datos espaciales y desarrollo de los metadatos», comunicación presentada en *I Jornadas Ibéricas de Infraestruturas de Dados Espaciais*, Lisboa, 2010, disponible en la dirección de internet: http://www.idee.es/resources/presentaciones/JIIDE10/ID435_Marco_juridico_y_administrativo_de_la_geoinformacion.pdf

Gamero Casado, E. y Valero Torrijos, J. (Coords.): *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 3ª edición de 2010

Gómez Manresa, Mº F.: «Las tecnologías de la información y comunicación y el urbanismo. En especial, la necesaria aplicación al ámbito urbanístico de la normativa ambiental», en *Revista Aranzadi de Derecho Ambiental*, nº 13 (2008), pp. 157-174.

Guichot, E. (Coord.): *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013, dse 9 de diciembre*, Tecnos, Madrid, 2014.

Martínez Gutiérrez, R.: «Nuevas tecnologías y policía de aguas», en *Revista Aranzadi de Derecho Ambiental*, nº 16 (2009), pp. 269-287.

Pigrau Solé, A. (coord.): *Acceso a la información, participación pública y acceso a la justicia en materia de medio ambiente: diez años del Convenio de Aarhus*, 2008, Barcelona, Atelier.

Razquin Lizarraga, J. A. y Ruiz de Apodaca Espinosa, Á.: *Información, Participación y Justicia en Materia de Medio Ambiente. Comentario sistemático a la Ley 27/2006, de 18 de julio,* 2007, Cizur Menor, Thomson-Aranzadi.

Rázquin Lizarraga, M. M.: *La confidencialidad de los datos empresariales en poder de las Administraciones Públicas (Unión Europea y España),* Iustel, Madrid, 2013..

Pomfret, K. D.: *The Importance of a Legal and Policy Framework for Spatial Data* (2009).

Sánchez Jordán, M. H.: «Información territorial y seguridad jurídicoa: cuestiones problemáticas», comunicación presentada a las *III Jornadas Ibéricas de Infraestructura de la Información de Dartos Espaciales*, Madrid, octubre de 2012, disponible en la siguiente página de internet: http://www.idee.es/resources/presentaciones/JIIDE12/miercoles/C19.Articulo.pdf

Sánchez Ortega, I. y De la Cueva, J.: «¿Son «libres» los geodatos «libres»? La *Open Database Lincese* y el punto de vista de *OpenStreetMap*, en comunicación presentada a las *VI Jornadas Técnicas de la Infraestructura de Datos de España*, Murcia, junio de 2009, disponible en la página de internet: http://www.idee.es/resources/presentaciones/GTIDEE_Murcia_2009/ARTICULOS_JIDEE2009/Articulo-21.pdf

Direcciones de internet:

- Unión Europea. *Infraestructure for Spatial Information in the European Community*: http://inspire.ec.europa.eu/
- Unión Europea, Agencia Europea de Medio Ambiente: aplicaciones móviles: http://www.eea.europa.eu/mobile
- España. Consejo Superior Geográfico de España: Infraestructura de datos espaciales (IDEE): http://www.idee.es
- Estados Unidos de América: «Open Initiative» de la *Environmental Protection Agency*: http://www2.epa.gov/open
- Estados Unidos de América: *Centre for Spatial Law and Policy*. http://www.spatiallaw.com/
- Universidad de Valencia y Red de Especialistas en Derecho de las Nuevas Tecnologías de la Información y Comunicación: *I Congreso Internacional de Open Government*: http://www.congresointernacionalogov.com/

REGULACIÓN COMÚN DE LA PRESENTACIÓN TELEMÁTICA DE DECLARACIONES TRIBUTARIAS

Rafael Oliver Cuello
Abogado. Asesor Fiscal. Profesor Consultor de Fiscalidad
Universitat Oberta de Catalunya

RESUMEN: La Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones y declaraciones informativas de naturaleza tributaria, desarrolla la regulación de la presentación telemática de declaraciones tributarias. Básicamente, esta Orden establece una regulación común del sistema de presentación telemática de las autoliquidaciones y declaraciones informativas, refundiendo en una sola norma la regulación existente, evitando la dispersión normativa. Esta regulación común, sin duda, contribuirá a aclarar y simplificar la aplicación de las normas tributarias en este campo tan novedoso y cambiante, mejorando la seguridad jurídica. Mediante esta Orden ministerial se regulan, entre otros temas, las formas de presentación de las autoliquidaciones (incluido el nuevo sistema de firma con clave de acceso en un registro previo como usuario, denominado PIN 24 horas), las autoliquidaciones de presentación electrónica obligatoria por Internet, el procedimiento general para la presentación electrónica por Internet de las autoliquidaciones, las formas de presentación de las declaraciones informativas, las declaraciones informativas de presentación electrónica obligatoria por Internet (entre otras, la polémica declaración telemática obligatoria del resumen anual del impuesto sobre el valor añadido), así como el procedimiento para la presentación electrónica por Internet de las declaraciones informativas.

PALABRAS CLAVE: Declaración tributaria, autoliquidación, presentación telemática, administración electrónica, impuestos.

1. LA ORDEN HAP/2194/2013, DE 22 DE NOVIEMBRE, POR LA QUE SE ESTABLECE LA REGULACIÓN COMÚN DE LA PRESENTACIÓN TELEMÁTICA DE DECLARACIONES TRIBUTARIAS

La Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimiento y las condiciones generales para la presentación de determinadas autoliquidaciones y declaraciones informativas de naturaleza tributaria, establece una regulación común del sistema de presentación telemática de las autoliquidaciones y declaraciones informativas.[1]

1 A la presentación de declaraciones, autoliquidaciones y comunicaciones tributarias se refiere el art. 29.2.c de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT) como una obli-

Se trata de una norma que refunde la regulación existente, evitando la dispersión normativa y contribuyendo, a nuestro juicio, a aclarar y simplificar la aplicación de las normas tributarias, lo cual repercute en una mayor seguridad jurídica.

En nuestra opinión, la principal aportación de esta Orden es, pues, el establecimiento de una regulación común del sistema de presentación telemática de las autoliquidaciones y declaraciones informativas tributarias, que hasta el momento se encontraba diseminada en diversas disposiciones normativas. No obstante, esta Orden es más conocida en la opinión pública por dos novedades introducidas por la misma y que serán objeto de comentario más adelante: el sistema de firma electrónica no avanzada del PIN 24 horas y la obligación de presentación por Internet de la declaración resumen anual del impuesto sobre el valor añadido (IVA).

De acuerdo con el preámbulo de esta Orden ministerial, «en el ámbito de la presentación de autoliquidaciones y declaraciones informativas, la constante evolución de la tecnología asociada a Internet ha venido a demostrar las indudables ventajas que presenta la vía telemática frente a la utilización de otros medios, como son los modelos de presentación en papel, dado que permite evitar a los obligados desplazamientos, colas o esperas innecesarias, además de agilizar considerablemente la gestión de los tributos».

Prosigue el preámbulo de esta Orden señalando que «en consonancia con esta línea de actuación, es objetivo primordial de esta Orden reducir al máximo posible la presentación en papel de las autoliquidaciones y declaraciones informativas mientras se potencian nuevas vías de presentación como son las basadas en los sistemas de firma electrónica no avanzada (…), así como la presentación de autoliquidaciones mediante papel impreso generado exclusivamente mediante la utilización del servicio de impresión desarrollado a estos efectos por la Agencia Estatal de Administración Tributaria en su sede electrónica (pre-declaración) o, en el supuesto de la declaración resumen anual del IVA y la declaración anual de operaciones con terceras personas de entidades a las que sea de aplicación la Ley 49/1960, de 21 de junio, sobre la Propiedad Horizontal, mediante el envío de un mensaje SMS cuando haya sido obtenida por medio del programa de ayuda elaborado por la Agencia Estatal de Administración Tributaria utilizando el servicio de impresión a través de su sede electrónica».

Las disposiciones de esta Orden son de aplicación a los principales modelos de autoliquidación, como, por ejemplo, los del impuesto sobre la renta de las personas físicas (IRPF), el impuesto sobre sociedades (IS), el IVA, el impuesto sobre el patrimonio (IP) o diversas tasas estatales. También son de aplicación en la mayoría de declaraciones in-

---

gación tributaria formal, que puede cumplirse por vía telemática. Véase sobre este tema DELGADO GARCÍA, Ana María: «La obligatoriedad de la presentación telemática de declaraciones tributarias», Revista de Información Fiscal, núm. 96, 2009, págs. 43-69. Y también ROVIRA FERRER, Irene: Los deberes de información y asistencia de la administración tributaria en la sociedad de la información, Bosch, Barcelona, 2011, págs. 187-239.

formativas, como, por ejemplo, la declaración resumen anual de retenciones e ingresos a cuenta del IRPF o del IS, la declaración anual de operaciones con terceras personas, la declaración resumen anual del IVA o la declaración informativa sobre bienes y derechos situados en el extranjero.

En su art. 1, la Orden HAP/2194/2013 establece el ámbito objetivo de aplicación, enumerando los modelos de autoliquidación y declaraciones informativas a los que es de aplicación. Por lo tanto, todos aquellos modelos que no estén citados en dicho precepto se regirán por su normativa de presentación y pago específica.

Sin embargo, quedan fuera del ámbito de aplicación de esta Orden las declaraciones aduaneras, las autoliquidaciones referentes a los impuestos especiales y las de los no residentes (modelos 210, 211 y 213) por tener una normativa específica que amplía el ámbito obligatorio de su presentación telemática. También quedan fuera las autoliquidaciones que se deben realizar solo con carácter ocasional (modelos 308 de solicitud de devolución del recargo de equivalencia, 309 de declaración-liquidación no periódica del IVA y 341 de solicitud de reintegro de compensaciones), las referentes a la tasa judicial (modelos 695 y 696), las declaraciones censales, así como las autoliquidaciones con competencia específica de gestión por las comunidades autónomas (por ejemplo, el impuesto sobre transmisiones patrimoniales y actos jurídicos documentados o el impuesto sobre sucesiones y donaciones).

2. FORMAS DE PRESENTACIÓN DE LAS AUTOLIQUIDACIONES. EL PIN 24 HORAS

Se establece en el art. 2 de la Orden HAP/2194/2013 que la presentación de las autoliquidaciones podrá ser realizada de cuatro formas distintas.

En primer lugar, mediante la presentación electrónica por Internet, la cual podrá ser efectuada con una firma electrónica avanzada o bien, en el caso de obligados tributarios personas físicas, mediante el sistema de firma con clave de acceso en un registro previo como usuario, establecido y desarrollado en la Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada. Se exceptúa de este último supuesto la presentación electrónica obligatoria de autoliquidaciones del IVA por parte de obligados tributarios cuyo período de liquidación coincida con el mes natural, que en todo caso deberá realizarse con firma electrónica avanzada.[2]

2 Según la Disposición Transitoria Única de la Orden HAP/2194/2013, hasta el 1 de enero de 2015 no será aplicable lo dispuesto respecto de la presentación electrónica con firma no avanzada a los siguientes modelos de autoliquidación, manteniendo sus actuales formas de presen-

En segundo lugar, la presentación podrá realizarse por medio de papel impreso generado exclusivamente por la utilización del servicio de impresión desarrollado a estos efectos por la Agencia Estatal de Administración Tributaria en su sede electrónica solo en el supuesto de los modelos de autoliquidación 111 y 115 (retenciones e ingresos a cuenta del IRPF), 130 y 131 (pagos fraccionados del IRPF), 136 (gravamen especial de determinadas loterías) y 303 (IVA).[3]

En tercer lugar, en las declaraciones del modelo 100 (IRPF) y del modelo 714 (IP), también podrán presentarse electrónicamente por Internet mediante la consignación del NIF del obligado tributario y del número de referencia del borrador o de los datos fiscales previamente suministrados por la Agencia Estatal de Administración Tributaria.

Y, en cuarto lugar, en relación con el IRPF, la presentación de la declaración también podrá realizarse en papel impreso a través del programa de ayuda o por el módulo de impresión correspondiente y, en los supuestos determinados en la orden ministerial de aprobación del modelo anual, mediante la confirmación o suscripción del borrador de declaración o bien por medio de la cumplimentación manual de la declaración.

---

tación: modelo 117 (IRPF, IS e IRNR. Retenciones e Ingresos a cuenta. Pago a cuenta. Rentas o ganancias patrimoniales obtenidas como consecuencia de las transmisiones o reembolsos de acciones y participaciones representativas del capital o del patrimonio de las instituciones de inversión colectiva); modelo 123 (IRPF. Retenciones e ingresos a cuenta sobre determinados rendimientos del capital mobiliario. IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre determinadas rentas); modelo 124 (IRPF. IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre rendimientos del capital mobiliario y rentas derivadas de la transmisión, amortización, reembolso, canje o conversión de cualquier clase de activos representativos de la captación y utilización de capitales ajenos); modelo 126 (IRPF. IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre rendimientos del capital mobiliario y rentas obtenidas por la contraprestación derivada de cuentas en toda clase de instituciones financieras, incluyendo las basadas en operaciones sobre activos financieros); modelo 128 (IRPF. IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta. Rentas o rendimientos del capital mobiliario procedentes de operaciones de capitalización y de contratos de seguro de vida o invalidez) y modelo 216 (IRNR. Rentas obtenidas sin mediación de establecimiento permanente. Retenciones e ingresos a cuenta).

3 De acuerdo con lo previsto por la Disposición Transitoria Única de la Orden HAP/2194/2013, hasta el 1 de enero de 2015 no será aplicable lo dispuesto en relación con la presentación electrónica por Internet ni en relación con la presentación por medio de papel impreso generado exclusivamente por la utilización del servicio de impresión desarrollado a estos efectos por la Agencia Estatal de Administración Tributaria en su sede electrónica, a los siguientes modelos de autoliquidación, manteniendo hasta entonces sus actuales formas de presentación: modelo 115 (IRPF, IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre determinadas rentas o rendimientos procedentes del arrendamiento o subarrendamiento de inmuebles urbanos); modelo 130 (IRPF. Actividades económicas en estimación directa. Pago fraccionado. Declaración) y modelo 131 (IRPF. Actividades económicas en estimación objetiva. Pago fraccionado. Declaración).

En relación con el denominado PIN 24 horas, se trata del sistema de firma con clave de acceso en un registro previo como usuario, establecido y desarrollado en el anexo III de la Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada.

Según esta Resolución, el sistema consiste en la aportación por el ciudadano de determinados datos, conocidos solamente por él y la Agencia Estatal de Administración Tributaria, distintos de la clave o número de referencia, que sean requeridos para la realización, por vía electrónica, de determinados trámites o actuaciones que no impliquen acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación.

Mediante la aportación de los datos indicados, el ciudadano podrá acceder electrónicamente, a través de los canales que se encuentren disponibles en cada momento, a los trámites y actuaciones determinados para los que se haya habilitado este sistema. La validez del sistema podrá estar limitada temporalmente en función de los plazos asociados a los trámites o actuaciones para los que se haya determinado su utilización. La utilización del sistema descrito por parte del ciudadano implicará el consentimiento para su uso como sistema de firma electrónica.

Finalmente, según el anexo III de esta Resolución, cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la citada Resolución, la Agencia Estatal de Administración Tributaria generará automáticamente un acuse de recibo o recibo de presentación.[4]

Con base en la regulación citada, se ha establecido el denominado PIN 24 horas. Este sistema se podrá utilizar por personas físicas, siempre que no estén obligadas a la presentación obligatoria por Internet con certificado electrónico. En consecuencia, en un primer momento, sus principales destinatarios son los autónomos que deben realizar presentaciones periódicas de autoliquidaciones así como la presentación de declaraciones informativas siempre que no excedan de 15 o 100 registros. Conviene destacar también, como novedad, la posibilidad de que se podrá utilizar para la presentación del modelo 720 (declaración informativa sobre bienes y derechos situados en el extranjero) que no exceda de 100 registros (hasta ahora únicamente se permitía presentarlo con certificado electrónico).

4 Véase, asimismo, la Resolución de 4 de marzo de 2014, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre asistencia a los obligados tributarios y ciudadanos en su identificación telemática ante las entidades colaboradoras con ocasión del pago de deudas por el procedimiento de cargo en cuenta, mediante el sistema de firma no avanzada con clave de acceso en un registro previo (PIN 24 horas).

El primer paso para la utilización del PIN 24 horas consiste en el registro previo en el sistema. Se realiza una sola vez por cualquiera de las siguientes vías: a) Respondiendo a la invitación a registrarse que realizará la Agencia Estatal de Administración Tributaria mediante el envío de cartas de comunicación al colectivo principalmente afectado, utilizando para ello el Código Seguro de Verificación (CSV)[5] que figura en la carta; b) Solicitando a través de Internet el envío al domicilio fiscal de una carta con CSV que permita realizar el registro; c) Utilizando el certificado electrónico; d) Presencialmente en las oficinas de la Agencia Estatal de Administración Tributaria.

En el proceso de registro se solicitará al contribuyente un número de teléfono móvil, la fecha de caducidad del documento nacional de identidad (DNI) o, en su defecto, otra fecha significativa, además de un código IBAN.[6] En el caso de ciudadanos con certificado electrónico reconocido se requerirá un número de teléfono móvil y la fecha de caducidad.

El segundo paso para la utilización del PIN 24 horas consiste en la identificación y autenticación. Una vez registrado en el sistema, cuando el contribuyente desee realizar algún trámite, deberá acceder a la sede electrónica de la Agencia Estatal de Administración Tributaria. A continuación, deberá solicitar un PIN 24 horas. Para ello deberá consignar el Número de Identificación Fiscal (NIF), la fecha de caducidad del DNI y una clave de identificación de cuatro caracteres que definirá el contribuyente para cada solicitud del PIN 24 horas. Recibirá el PIN mediante un SMS remitido al teléfono móvil, comunicado en la fase de registro, que se podrá utilizar hasta las 2:00 del día siguiente al de la recepción del mensaje.

---

5 En relación con los sistemas de Código Seguro de Verificación, establece el art. 20.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, que «la Administración General del Estado y sus organismos públicos vinculados o dependientes podrán utilizar sistemas de Código Seguro de Verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente». Por su parte, el apartado 2 del mismo precepto señala que «el sistema de Código Seguro de Verificación deberá garantizar, en todo caso: a) El carácter único del código generado para cada documento. b) Su vinculación con el documento generado y con el firmante. c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento».

6 El Código Internacional de Cuenta Bancaria o International Bank Account Number (IBAN) es un código alfanumérico que identifica una cuenta bancaria determinada en una entidad financiera. A través del código IBAN se identifica el país, la entidad, la oficina y la cuenta bancaria. Se trata de un estándar (EBS204) del Comité Europeo de Estándares Bancarios, cuyo objetivo es facilitar el tratamiento automático de pagos y cobros transfronterizos.

3. AUTOLIQUIDACIONES DE PRESENTACIÓN ELECTRÓNICA OBLIGATORIA POR INTERNET

Como regla general, la presentación de autoliquidaciones tributarias por vía telemática es voluntaria, aunque en determinados supuestos y para determinados obligados tributarios la utilización de la vía telemática es obligatoria, en los términos previstos en el art. 98.4 LGT.[7]

De acuerdo con el art. 3 de la Orden HAP/2194/2013, la presentación electrónica por Internet con firma electrónica avanzada tendrá carácter obligatorio para aquellos obligados tributarios que tengan el carácter de administración pública o bien se encuentren inscritos en el Registro de Grandes Empresas, bien estén adscritos a la Delegación Central de Grandes Contribuyentes o bien tengan la forma de sociedad anónima o sociedad de responsabilidad limitada.

Asimismo, la presentación electrónica por Internet con firma electrónica avanzada tendrá carácter obligatorio, en cualquier caso, en las autoliquidaciones del IVA de aquellos obligados tributarios cuyo período de liquidación coincida con el mes natural, así como en el supuesto del modelo 430 (impuesto sobre primas de seguros), cualquiera que sea el obligado a su presentación.

También tendrá carácter obligatorio la presentación electrónica por Internet en las presentaciones correspondientes al IRPF y al IP a realizar por las personas físicas que deban efectuar la declaración del impuesto sobre el patrimonio.

4. PROCEDIMIENTO GENERAL PARA LA PRESENTACIÓN ELECTRÓNICA POR INTERNET DE LAS AUTOLIQUIDACIONES

En el art. 6 de la Orden HAP/2194/2013 se regulan los sujetos habilitados para la presentación electrónica de autoliquidaciones (los obligados tributarios, sus representantes o los colaboradores sociales), así como las condiciones generales para dicha presentación electrónica (disponer de un NIF y de un certificado electrónico, así como la utilización de los formularios y programas informáticos para la cumplimentación de declaraciones).

En cuanto al momento de la presentación electrónica, se dispone que la transmisión electrónica de las autoliquidaciones con resultado a ingresar, cuando no se opte por la domiciliación bancaria como medio de pago, deberá realizarse en la misma fecha en que tenga lugar el ingreso resultante de aquellas. No obstante, en el caso de que existan

7 Véase al respecto OLIVER CUELLO, Rafael: Internet y tributos, Bosch, Barcelona, 2012, págs. 282-290. Y también LÓPEZ LUBIAN, José Ignacio: «Las presentaciones fiscales telemáticas de PYMES y profesionales», Ciss Carta Tributaria, núm. 4, 2009.

dificultades técnicas que impidan efectuar la transmisión electrónica en la misma fecha del ingreso, podrá realizarse dicha transmisión electrónica hasta el cuarto día natural siguiente al del ingreso. Y en aquellos casos en que se detecten anomalías de tipo formal en la transmisión electrónica de las declaraciones, dicha circunstancia se pondrá en conocimiento del presentador de la declaración por el propio sistema mediante los correspondientes mensajes de error, para que proceda a su subsanación.

Por otra parte, en el art. 7 de esta Orden se regula el procedimiento general para la presentación electrónica de las autoliquidaciones con resultado a ingresar cuando el pago no se realice mediante domiciliación bancaria. En el art. 8 se hace lo propio con el procedimiento para las autoliquidaciones con resultado a ingresar cuando el pago se realice mediante domiciliación bancaria. Y en el art. 9 se establece el procedimiento para las autoliquidaciones con solicitud de aplazamiento o fraccionamiento, compensación o con reconocimiento de deuda. Finalmente, el art. 10 se dedica al procedimiento para las autoliquidaciones con solicitud de pago mediante entrega de bienes del Patrimonio Histórico Español,[8] mientras que el art. 11 tiene por objeto el procedimiento para la presentación electrónica de autoliquidaciones con resultado a devolver, a compensar o negativas.

A continuación, procederemos a describir los tres procedimientos de presentación telemática de autoliquidaciones más generales, regulados en los arts. 7, 8 y 11 de esta Orden HAP/2194/2013.

8 Según la Disposición Transitoria Única de la Orden HAP/2194/2013, hasta el 1 de enero de 2015 no será aplicable lo dispuesto en los arts. 9 y 10 de esta Orden a los siguientes modelos de autoliquidación: modelo 115 (IRPF, IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre determinadas rentas o rendimientos procedentes del arrendamiento o subarrendamiento de inmuebles urbanos); modelo 123 (IRPF. Retenciones e ingresos a cuenta sobre determinados rendimientos del capital mobiliario. IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre determinadas rentas); modelo 124 (IRPF, IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre rendimientos del capital mobiliario y rentas derivadas de la transmisión, amortización, reembolso, canje o conversión de cualquier clase de activos representativos de la captación y utilización de capitales ajenos); modelo 126 (IRPF, IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta sobre rendimientos del capital mobiliario y rentas obtenidas por la contraprestación derivada de cuentas en toda clase de instituciones financieras, incluyendo las basadas en operaciones sobre activos financieros); modelo 128 (IRPF, IS e IRNR, establecimientos permanentes. Retenciones e ingresos a cuenta. Rentas o rendimientos del capital mobiliario procedentes de operaciones de capitalización y de contratos de seguro de vida o invalidez); modelo 130 (IRPF. Actividades económicas en estimación directa. Pago fraccionado. Declaración); modelo 131 (IRPF. Actividades económicas en estimación objetiva. Pago fraccionado. Declaración); modelo 216 (IRNR. Rentas obtenidas sin mediación de establecimiento permanente. Retenciones e ingresos a cuenta) y modelo 430 (Impuesto sobre primas de seguros. Declaración-Liquidación).

Respecto al procedimiento general para la presentación electrónica por Internet de las autoliquidaciones con resultado a ingresar, cuando el pago no se realice mediante domiciliación bancaria, en primer lugar, el obligado tributario o, en su caso, el presentador, deberá ponerse en contacto con la entidad colaboradora, ya sea por vía electrónica (directamente o a través de la sede electrónica de la Agencia Estatal de Administración Tributaria) o acudiendo a sus sucursales para realizar el pago de la cuota resultante.

Una vez realizado el ingreso, la entidad colaboradora proporcionará al obligado tributario o al presentador el recibo justificante de pago. En dicho recibo justificante de pago, en todo caso, deberá figurar el Número de Referencia Completo (NRC) asignado por la entidad colaboradora al ingreso realizado.

Tras efectuar la operación anterior, el obligado tributario o, en su caso, el presentador conectará con la sede electrónica de la Agencia Estatal de Administración Tributaria y accederá al trámite de presentación correspondiente a la autoliquidación que desea transmitir. Realizada dicha selección, cumplimentará el correspondiente formulario e introducirá el NRC proporcionado por la entidad colaboradora. Seguidamente, procederá a transmitir la autoliquidación con la firma electrónica generada al seleccionar el certificado previamente instalado en el navegador a tal efecto.[9]

En los supuestos de presentación de las autoliquidaciones bien mediante el sistema de firma con clave de acceso en un registro previo como usuario, bien mediante el número o números de referencia del borrador o datos fiscales, el obligado tributario deberá obtener el NRC de la entidad colaboradora de forma directa, por vía electrónica o bien acudiendo a sus oficinas, y proceder a transmitir la autoliquidación, sin necesidad de firma electrónica avanzada, mediante la consignación del NIF del obligado tributario, el NRC y la correspondiente clave de acceso o número de referencia del borrador o de los datos fiscales, previamente suministrados por la Agencia Estatal de Administración Tributaria.

Si la autoliquidación es aceptada, la Agencia Estatal de Administración Tributaria le devolverá en pantalla los datos de la autoliquidación con resultado a ingresar, validados con un CSV de 16 caracteres, además de la fecha y hora de la presentación. En el supuesto de que la presentación fuese rechazada, se mostrará en pantalla la descripción de los errores detectados. En este caso, se deberá proceder a subsanar los mismos, bien en el formulario de entrada, bien con el programa de ayuda con el que se generó el fichero, o repitiendo la presentación si el error fuese ocasionado por otro motivo. El obligado tributario o presentador deberá conservar la autoliquidación aceptada, así como el documento de ingreso debidamente validados con el correspondiente CSV.

9 En el caso de declaración conjunta del IRPF formulada por ambos cónyuges, deberá seleccionar adicionalmente la firma electrónica correspondiente al cónyuge. Si el presentador es colaborador social debidamente autorizado, se requerirá la firma electrónica correspondiente a su certificado electrónico.

En relación con el procedimiento para la presentación electrónica de autoliquidaciones con resultado a ingresar, cuando el pago se realice mediante domiciliación bancaria, en primer lugar, el obligado tributario o, en su caso, el presentador conectará con la sede electrónica de la Agencia Estatal de Administración Tributaria y accederá al trámite de presentación correspondiente a la autoliquidación que desea transmitir. Las personas o entidades que ostenten la condición de colaboradores sociales en la aplicación de los tributos podrán dar traslado por vía electrónica de las órdenes de domiciliación que previamente les hubieran comunicado los obligados tributarios en cuyo nombre actúan.

Una vez llevada a cabo dicha selección, se cumplimentará el formulario correspondiente consignando la orden de domiciliación y se introducirá el Código Internacional de Cuenta Bancaria (IBAN) de la cuenta en que se domicilie el pago. A continuación, se transmitirá la autoliquidación con la firma electrónica generada mediante el certificado electrónico utilizado.[10]

En los supuestos de presentación de las autoliquidaciones bien mediante el sistema de firma con clave de acceso en un registro previo como usuario, bien mediante el número o números de referencia del borrador o datos fiscales, el obligado tributario procederá a transmitir la autoliquidación, sin necesidad de firma electrónica avanzada, mediante la consignación del NIF del obligado tributario y la correspondiente clave de acceso o número de referencia del borrador o de los datos fiscales, previamente suministrados por la Agencia Estatal de Administración Tributaria.

Si la autoliquidación con orden de domiciliación es aceptada, la Agencia Estatal de Administración Tributaria devolverá en pantalla los datos de la misma y la codificación de la cuenta de domiciliación validada con un CSV, además de la fecha y hora de la presentación. El obligado tributario o el presentador deberán conservar la declaración aceptada y validada con el mencionado código electrónico.

En caso de que la presentación con orden de domiciliación fuera rechazada, se mostrará en pantalla la descripción de los errores detectados con el fin de que se pueda llevar a cabo la posterior subsanación de los mismos con el programa de ayuda con el que se generó el fichero, o en el formulario de entrada, o repitiendo la presentación si el error se hubiese originado por otras causas.

La Agencia Estatal de Administración Tributaria comunicará las órdenes de domiciliación de los obligados tributarios a las diferentes entidades colaboradoras, las cuales procederán a cargar en cuenta el importe domiciliado el último día del plazo de ingreso en periodo voluntario y a abonarlo en la cuenta restringida que corresponda. Una vez efectuado el adeudo de la domiciliación, la entidad colaboradora remitirá al obligado tributario el recibo justificante del pago realizado.

10 Si el presentador es un colaborador social debidamente autorizado, se requerirá la firma electrónica correspondiente a su certificado electrónico.

Por último, respecto al procedimiento para la presentación electrónica de autoliquidaciones con resultado a devolver, a compensar o negativas, en primer lugar, el obligado tributario o, en su caso, el presentador conectará con la sede electrónica de la Agencia Estatal de Administración Tributaria y accederá al trámite de presentación relativo a la autoliquidación que desea transmitir y seguidamente cumplimentará el formulario que corresponda.

A continuación, se procederá a transmitir la declaración con la firma electrónica generada mediante el certificado electrónico utilizado.[11] No obstante, en los supuestos de presentación de las autoliquidaciones bien mediante el sistema de firma con clave de acceso en un registro previo como usuario, bien mediante el número o números de referencia del borrador o datos fiscales, el obligado tributario también podrá proceder a transmitir la autoliquidación, sin necesidad de firma electrónica avanzada, mediante la consignación del NIF del obligado tributario y la correspondiente clave de acceso o número de referencia del borrador o de los datos fiscales, previamente suministrados por la Agencia Estatal de Administración Tributaria.

Si la autoliquidación es aceptada, la Agencia Estatal de Administración Tributaria devolverá en pantalla los datos de la misma, validados con un CSV, la fecha y la hora de la presentación. Tratándose de declaraciones o autoliquidaciones con resultado a devolver en las que el obligado tributario hubiera optado por percibir la devolución mediante transferencia, se incluirá la codificación de la cuenta designada a tal efecto. El obligado tributario o el presentador deberán conservar la autoliquidación aceptada y validada con el mencionado código electrónico.

En caso de que la presentación fuera rechazada, se mostrará en pantalla la descripción de los errores detectados con el fin de que se pueda llevar a cabo la posterior subsanación de los mismos con el programa de ayuda con el que se generó el fichero, o en el formulario de entrada, o repitiendo la presentación si el error se hubiese originado por otras causas.

5. FORMAS DE PRESENTACIÓN DE LAS DECLARACIONES INFORMATIVAS

De acuerdo con lo previsto por el art. 12 de la Orden HAP/2194/2013, la presentación de las declaraciones informativas podrá ser realizada de tres formas.

En primer lugar (y al igual que sucede con las autoliquidaciones), mediante la presentación electrónica por Internet, la cual podrá ser efectuada con una firma electró-

11 Si el presentador es un colaborador social debidamente autorizado, se requerirá la firma electrónica correspondiente a su certificado electrónico.

nica avanzada o bien, en el caso de obligados tributarios personas físicas, mediante el sistema de firma con clave de acceso en un registro previo como usuario, establecido y desarrollado en la citada Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria. Se exceptúa de este último supuesto la presentación electrónica obligatoria de la declaración resumen anual del IVA (modelo 390) por parte de obligados tributarios cuyo período de liquidación coincida con el mes natural, que en todo caso deberá realizarse con firma electrónica avanzada. Hay que tener en cuenta, asimismo, que la Agencia Estatal de Administración Tributaria limitará la presentación electrónica al sistema de firma con clave de acceso en un registro previo como usuario en función del número de registros que sean objeto de declaración.

En segundo lugar, la presentación electrónica de la declaración también se podrá efectuar mediante el envío de un mensaje SMS en el supuesto de la declaración resumen anual del IVA (modelo 390) y la declaración anual de operaciones con terceras personas (modelo 347) correspondiente a entidades a las que sea de aplicación la Ley 49/1960, de 21 de junio, sobre la Propiedad Horizontal, siempre que no exceda de 15 registros, que hayan sido obtenidas por medio del programa de ayuda elaborado por la Agencia Estatal de Administración Tributaria utilizando el servicio de impresión a través de su sede electrónica. Se exceptúa también la presentación electrónica obligatoria de la declaración resumen anual del IVA (modelo 390) por parte de obligados tributarios cuyo período de liquidación coincida con el mes natural.

Y, en tercer lugar, en todo caso, las declaraciones informativas que contengan más de 10.000.000 de registros también podrán presentarse en soporte directamente legible por ordenador de acuerdo con las características y condiciones señaladas en el art. 15 de esta Orden.

6. DECLARACIONES INFORMATIVAS DE PRESENTACIÓN ELECTRÓNICA OBLIGATORIA POR INTERNET. EN ESPECIAL, LA DECLARACIÓN RESUMEN ANUAL DEL IVA

La presentación electrónica por Internet con firma electrónica avanzada tendrá carácter obligatorio, según establece el art. 13 de esta Orden, para todas las declaraciones informativas de aquellos obligados tributarios que, bien tengan el carácter de administración pública, bien estén adscritos a la Delegación Central de Grandes Contribuyentes o a alguna de las Unidades de Gestión de Grandes Empresas de la AEAT, o bien tengan la forma de sociedad anónima o sociedad de responsabilidad limitada.

También tendrá carácter obligatorio en el supuesto de la declaración resumen anual del IVA (modelo 390) correspondiente a obligados tributarios cuyo período de liquidación coincida con el mes natural; en la declaración resumen anual de las retenciones e ingresos a cuenta sobre rendimientos del capital mobiliario y rentas derivadas de la transmisión, amortización, reembolso, canje o conversión de cualquier clase de activos

representativos de la captación y utilización de capitales ajenos (modelo 194); y en la declaración resumen anual del impuesto sobre las primas de seguros (modelo 480), cualquiera que sea el obligado a su presentación.

Finalmente, en el supuesto de obligados tributarios personas físicas y en relación con la declaración informativa sobre bienes y derechos situados en el extranjero (modelo 720), será obligatoria la presentación electrónica por Internet, pudiendo utilizar para ello firma electrónica avanzada o bien el sistema de firma con clave de acceso en un registro previo como usuario. Se exceptúan también los obligados tributarios personas físicas cuyo período de liquidación coincida con el mes natural en la presentación electrónica obligatoria de la declaración resumen anual del IVA (modelo 390), que tendrán que utilizar en todo caso la firma electrónica avanzada.

En relación con la obligación de presentación electrónica por Internet de la declaración del resumen anual del IVA (modelo 390), la Defensora del Pueblo, el 6 de febrero de 2014, ha solicitado a la Agencia Estatal de Administración Tributaria que no obligue a la presentación del IVA de forma telemática y permita su presentación en papel, como se hacía hasta el momento, tras recibir quejas por la obligación de presentar la declaración del IVA de forma telemática exclusivamente.

Según la Defensora del Pueblo, los ciudadanos manifiestan que ahora, para poder cumplir con sus obligaciones tributarias, necesitan medios que no están a su alcance, como ordenador personal, conexión a Internet o teléfono móvil y conocimientos de informática. Las denuncias contra el nuevo sistema, a su entender, provienen de ciudadanos que no están en condiciones o les resulta muy difícil hacer estos trámites por ordenador, bien por su edad o por el pequeño volumen de su negocio o trabajo, y les obliga a costear los servicios de un tercero para cumplir con su obligación fiscal.

La Defensora del Pueblo también ha solicitado a la Agencia Estatal de Administración Tributaria que instale puestos informáticos, asistidos por personal de la Agencia, para ayudar y asesorar a los ciudadanos que quieran presentar sus autoliquidaciones y declaraciones por vía telemática. También ha recibido quejas relativas a fallos en el sistema de presentación, problemas a la hora de descargar el programa y dificultades para solicitar información telefónica. Por estos motivos, la Defensora del Pueblo ha recomendado que no se incoen procedimientos sancionadores por la presentación incorrecta de los modelos hasta que no se garantice que el sistema funciona sin errores.

La Agencia Estatal de Administración Tributaria, por su parte, ha concluido la campaña de presentación de la declaración anual de IVA (modelo 390), la primera en la que era obligatorio hacerlo de forma telemática exclusivamente, con un total de 3.366.000 declaraciones registradas, 249.000 más que al cierre de la campaña del año anterior, lo que supone un incremento del 8%.

De esta forma, el Ministerio de Hacienda ha destacado que la obligatoriedad de presentar la declaración por Internet, a pesar de las quejas que ha suscitado y los proble-

mas que han denunciado diversas organizaciones, ha permitido acelerar la tramitación del resumen anual de IVA. Además, la Agencia Estatal de Administración Tributaria indica que más de 403.000 de estas declaraciones se han realizado con el nuevo sistema de firma electrónica del denominado PIN 24 horas, y resalta el mayor empleo del certificado electrónico por parte del contribuyente.

Según datos del Ministerio de Hacienda, durante la campaña del resumen anual de IVA, que concluyó el 30 de enero de 2014, la Agencia Estatal de Administración Tributaria reforzó la información y asistencia en oficina, incluyendo en las dos últimas semanas un servicio de ayuda personalizada para los colectivos que consideró más sensibles ante la obligación de presentación telemática, que fue utilizado por un 21% de los contribuyentes. Previamente, a lo largo del mes de diciembre de 2013, la Agencia Estatal de Administración Tributaria remitió más de un millón de cartas informando a los contribuyentes sobre la obligación de presentación telemática y las distintas fórmulas que podían utilizar para cumplimentar y presentar estas declaraciones informativas.

Por otra parte, la sala de lo contencioso-administrativo de la Audiencia Nacional ha admitido a trámite un recurso interpuesto, el 24 de enero de 2014, por el Consejo General de la Abogacía Española (CGAE) contra la Orden HAP/2194/2013. En el recurso se pide la adopción de la medida cautelar de suspensión de la ejecución de la entrada en vigor de la orden ministerial recurrida.

Según la opinión del CGAE, «la citada Orden ministerial resulta lesiva para los legítimos intereses del CGAE como máxime representante de la Abogacía Española y para los abogados colegiados en los Colegios de Abogados de España que pudieran tener la obligación tributaria de presentar estas autoliquidaciones y declaraciones informativas que señala esta Orden en su artículo 1». En este sentido, entiende que «la Orden que ahora se recurre podría vulnerar la citada Ley 11/2007, por cuanto que el que una persona física tenga reconocido el derecho a relacionarse con la administración por medios electrónicos, nada impide, en cambio, a que su imposición como obligación debe venir justificada siempre sobre la base, como dice la citada Ley 11/2007, de la concurrencia en el sujeto de capacidad económica o técnica, dedicación profesional u otros motivos acreditados que garanticen el acceso y disponibilidad a los medios tecnológicos».

Se trata, por consiguiente, de dilucidar si el establecimiento de esta obligación afecta a sujetos con la suficiente capacidad económica o técnica o dedicación profesional para tener acceso y disponibilidad a los nuevos medios tecnológicos, circunstancias que, a nuestro juicio, se produce en el caso de las autoliquidaciones y declaraciones informativas tributarias incluidas en la Orden HAP/2194/2013, sobre todo teniendo en cuenta las facilidades de realización de trámites por Internet que se regulan en la propia Orden, como, por ejemplo, el denominado PIN 24 horas.

En definitiva, nos hallamos ante la polémica y discutible cuestión de la velocidad con la que deben establecerse obligaciones de empleo de Internet para relacionarse con las administraciones públicas, en general, y con la administración tributaria, en particu-

lar. En este asunto, a nuestro juicio, se deben ponderar, por un lado, los posibles inconvenientes que se puedan ocasionar a los obligados tributarios y, por el otro, las mejoras en la eficiencia de la administración tributaria, la aplicación de los tributos más efectiva y el incremento de la lucha contra el fraude que puede suponer el uso generalizado de las tecnologías de la información y la comunicación en las relaciones administrativas tributarias.

En cualquier caso, entendemos que la imposición de la obligación de presentación electrónica de autoliquidaciones y declaraciones informativas tributarias a determinados sujetos siempre debe ir acompañada del establecimiento de facilidades para el cumplimiento de las obligaciones tributarias (como ha sucedido con esta Orden), de una intensa campaña informativa sobre los nuevos deberes tributarios, así como de una flexibilidad en la aplicación de las nuevas obligaciones, evitando, en la medida de lo posible, acudir a la imposición de sanciones tributarias.

7. PROCEDIMIENTO PARA LA PRESENTACIÓN ELECTRÓNICA POR INTERNET DE LAS DECLARACIONES INFORMATIVAS

En el art. 16 de esta Orden se regulan de forma idéntica a las autoliquidaciones los sujetos habilitados para la presentación electrónica de declaraciones informativas, las condiciones generales para dicha presentación electrónica y los supuestos en que se detecten anomalías de tipo formal en la transmisión electrónica de las declaraciones.

La presentación electrónica por Internet de las declaraciones informativas a través de la sede electrónica de la Agencia Estatal de Administración Tributaria podrá ser efectuada por los obligados tributarios o, en su caso, sus representantes legales; por aquellos representantes voluntarios de los obligados tributarios con poderes o facultades para presentar electrónicamente en nombre de los mismos declaraciones y autoliquidaciones ante la Agencia o representarles ante esta; o por las personas o entidades que ostenten la condición de colaboradores sociales en la aplicación de los tributos.

El obligado tributario deberá disponer de NIF y estar identificado, con carácter previo a la presentación, en el Censo de Obligados Tributarios. Para efectuar la presentación electrónica utilizando una firma electrónica avanzada, el obligado tributario deberá disponer de un certificado electrónico.

Cuando la presentación electrónica mediante firma electrónica avanzada se realice por apoderados o por colaboradores sociales debidamente autorizados, serán estos quienes deberán disponer de su certificado electrónico. Para efectuar la presentación electrónica, el obligado tributario o, en su caso, el presentador, deberá generar previamente un fichero con la declaración a transmitir.

En aquellos casos en que se detecten anomalías de tipo formal en la transmisión electrónica de las declaraciones, dicha circunstancia se pondrá en conocimiento del pre-

sentador de la declaración por el propio sistema mediante los correspondientes mensajes de error, para que proceda a su subsanación.

Finalmente, en el art. 17 de esta Orden se establece el procedimiento para la presentación electrónica por Internet de las declaraciones informativas. Y en el art. 18 se hace lo propio con el procedimiento para la presentación electrónica por Internet de documentación complementaria a las autoliquidaciones y declaraciones informativas.

En relación con el procedimiento para la presentación electrónica por Internet de las declaraciones informativas, en primer lugar, el obligado tributario o, en su caso, el presentador, se pondrá en comunicación con la sede electrónica de la Agencia Estatal de Administración Tributaria en Internet y seleccionará el modelo a transmitir. A continuación, procederá a transmitir la correspondiente declaración con la firma electrónica generada al seleccionar el certificado previamente instalado en el navegador a tal efecto.[12]

Salvo en los supuestos señalados en el art. 13.1 de esta Orden en los que sea obligatoria la presentación con firma electrónica avanzada, la presentación electrónica por Internet de la declaración informativa también podrá realizarse mediante el sistema de firma con clave de acceso en un registro previo como usuario o mediante el envío de un mensaje SMS en el supuesto de la declaración resumen anual del IVA (modelo 390) y de la declaración anual de operaciones con terceras personas (modelo 347), correspondiente a entidades a las que sea de aplicación la Ley 49/1960, de 21 de junio, sobre la Propiedad Horizontal.

Si la declaración es aceptada, la Agencia Estatal de Administración Tributaria le devolverá en pantalla los datos de registro, validados con un CSV de 16 caracteres, además de la fecha y hora de presentación. En el supuesto de que la presentación fuera rechazada, se mostrará en pantalla un mensaje con la descripción de los errores detectados, debiendo proceder a la subsanación de los mismos. El obligado tributario, o en su caso, el presentador deberá conservar la declaración aceptada con el correspondiente CSV.

Por último, tras el proceso de validación de los datos suministrados, se ofrecerá, en su caso, al obligado tributario la información individualizada de los errores detectados en las declaraciones para que pueda proceder a su corrección. En caso de que no se hayan subsanado los defectos observados, se podrá requerir al obligado para que, en el plazo de 10 días, contados a partir del día siguiente al de la notificación del requerimiento, subsane los defectos de que adolezca. Transcurrido dicho plazo sin haber atendido el requerimiento, de persistir anomalías que impidan a la administración tributaria el conocimiento de los datos, se tendrá, en su caso, por no cumplida la obligación correspondiente y se procederá al archivo sin más trámite.

12 Si el presentador es una persona o entidad autorizada a presentar declaraciones en representación de terceras personas, se requerirá una única firma, la correspondiente a su certificado.

En aquellos supuestos en que, por razones de carácter técnico, no fuera posible efectuar la presentación por Internet en el plazo establecido reglamentariamente para cada declaración informativa, dicha presentación podrá efectuarse durante los cuatro días naturales siguientes al de finalización de dicho plazo.

8. BIBLIOGRAFÍA

Delgado García, Ana María (2009). «La obligatoriedad de la presentación telemática de declaraciones tributarias». *Revista de Información Fiscal* (núm. 96).

López Lubian, José Ignacio (2009). «Las presentaciones fiscales telemáticas de PYMES y profesionales». *Ciss Carta Tributaria* (núm. 4).

Oliver Cuello, Rafael (2012). *Internet y tributos*. Barcelona: Bosch.

Rovira Ferrer, Irene (2011). *Los deberes de información y asistencia de la administración tributaria en la sociedad de la información*. Barcelona: Bosch.

LA INCORPORACIÓN DE LAS TIC EN EL ÁMBITO TRIBUTARIO: UN NUEVO MODELO DE ADMINISTRACIÓN

Irene Rovira Ferrer
Profesora de Derecho Financiero y Tributario
Universitat Oberta de Catalunya

RESUMEN: Uno de los ámbitos de nuestro país que más se ha visto afectado por la incorporación de las Tecnologías de la Información y la Comunicación es el de la Administración Pública y, en especial, el de la Administración tributaria, pues, como es sabido, se ha convertido en todo un referente por excelencia tanto desde el punto de vista nacional como internacional. En concreto, aquellas primeras previsiones genéricas sobre la posibilidad de incorporar los nuevos medios y técnicas, contempladas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico del Procedimiento Administrativo Común, y, esencialmente, en la Ley 58/2003, de 17 de diciembre, General Tributaria, se han convertido hoy en una completa sede electrónica de la Agencia Estatal de la Administración Tributaria y en la presencia en Internet de la práctica totalidad de las Administraciones tributarias autonómicas y locales, lo que ha derivado en la informatización de la mayor parte de procedimientos, en una nueva forma de funcionamiento y, en último término, en un nuevo modelo de Administración. Así pues, el objeto del presente trabajo es la elaboración de un análisis general sobre la incorporación de las TIC en el seno de la Administración tributaria española, con el fin de poner de manifiesto los cambios y consecuencias más importantes que ha conllevado para poder efectuar su valoración.

PALABRAS CLAVE: Tecnologías de la Información y la Comunicación, Administración tributaria, Administración electrónica, sede electrónica, modelo administrativo.

1. INTRODUCCIÓN

Como no podía ser de otro modo, la instauración de la sociedad de la información y el conocimiento obligó a las Administraciones Públicas a tomar conciencia de la relevancia del uso de las Tecnologías de la Información y la Comunicación (TIC) y a apostar decididamente por su incorporación, pues su principal razón de ser (el servicio a los ciudadanos) exigía que se adaptaran al paulatino asentamiento de esta nueva realidad y, como es lógico, a las nuevas necesidades.

Asimismo, la introducción de las TIC se hizo imprescindible para poder garantizar la propia viabilidad del sistema administrativo en general, y es que, tras la pluralización de los intereses sociales que caracteriza la nueva sociedad, las Administraciones Públicas se encontraron con la difícil disyuntiva de afrontar los nuevos y numerosos retos con la misma cantidad de recursos públicos, lo que sólo resultaba posible con la potenciación

de la colaboración de los ciudadanos y con el aprovechamiento de las ventajas que ofrece el uso de los nuevos medios y técnicas.

En consecuencia, el aumento de eficiencia, eficacia y calidad de la actividad de la Administración no sólo dependía de la informatización de los diferentes procedimientos, sino que también exigía los cambios organizativos, funcionales y políticos necesarios para optimizar los esquemas de servicio público y para propiciar una mayor interacción con la ciudadanía, de forma que el camino hacia la e-Administración, más que la ampliación de vías, medios y recursos administrativos, entrañaba una auténtica reforma institucional.

Y justamente esta reforma es la que, como parte de la Administración Pública, se ha vivido en el ámbito tributario, donde, por sus propias características y ventajas inherentes, la incorporación de las TIC ha tenido un mayor desarrollo tanto normativo como material.

En concreto, en función de las principales líneas de actuación, el proceso transformador a consecuencia de las TIC que se ha experimentado en el seno de la Administración tributaria puede dividirse, a grandes rasgos, en tres fases fundamentales: una primera basada en la incorporación de los recursos tecnológicos, una segunda concretada en la adaptación de la normativa y una tercera destinada a conseguir la plena inclusión digital.

Así, partiendo de las mismas, el objetivo del presente trabajo es poner de manifiesto las principales características que ha tenido el proceso hacia la eAdministración tributaria, analizando especialmente una de las mayores consecuencias que ha comportado su aparición: la aparición de un nuevo modelo de Administración.

2. LA INCORPORACIÓN DE LOS RECURSOS TECNOLÓGICOS EN LA ADMINISTRACIÓN TRIBUTARIA

Con carácter general, podría decirse que la primera etapa hacia la Administración electrónica tributaria arrancó en España a principios de los años 80 con una fuerte inversión para la informatización de toda la actividad administrativa, llegando a su punto álgido con la incorporación de aplicaciones de carácter automatizado y, como es lógico, con la instauración de sedes electrónicas (es decir, de auténticas extensiones virtuales de las oficinas de la Agencia Tributaria operativas las 24 horas de los 365 días del año)[1].

1 Al respecto, en palabras de Cerrillo, puede definirse la sede electrónica como «una nueva figura que introduce la LAECSP en nuestro ordenamiento jurídico llamada a jugar un papel central en las relaciones entre los ciudadanos y las Administraciones Públicas a través de medios electrónicos, al ser configurada como la puerta de entrada a las Administraciones Públicas, a la información que difunden y los servicios que prestan a través de medios electrónicos». (Cerrillo Martínez, A. (2010). La difusión de información pública a través de medios electrónicos: claroscuros de la Ley de acceso electrónico de los ciudadanos a los servicios públicos (pág. 385). En

Así, ya sea con webs propias o compartidas, puede afirmarse que la práctica totalidad de Administraciones tributarias ya tiene actualmente presencia en Internet (donde, además de la consulta de información, se permite la realización de trámites y procedimientos electrónicos y la obtención de servicios en línea), siendo la estrella, como es lógico, la sede electrónica de la Agencia Estatal de la Administración Tributaria (AEAT –disponible en la web http://www.agenciatributaria.es/–)[2].

No obstante, en relación con el desarrollo de las diversas aplicaciones instauradas, deben destacarse negativamente los fuertes desequilibrios que se observan, tanto entre los distintos niveles administrativos como entre las propias Administraciones territoriales (ya sean autonómicas o, sobre todo, locales). Así, y a pesar de las evidentes diferencias entre las características y los recursos de las distintas Administraciones, conviene subrayar la necesidad de conseguir la máxima homogenización, pues la clave para el definitivo asentamiento de la Administración electrónica se encuentra, sin lugar a dudas, en la interconexión y la coordinación de toda la Administración.

En este sentido, conviene tener presente que la actuación conjunta es la única forma de acabar con las fuertes desigualdades y de conseguir el mayor desarrollo en las distintas aplicaciones de las TIC, y es que la elaboración de planificaciones estratégicas para conseguir el avance común es la única manera de diseñar las mejores iniciativas (con base en los diferentes resultados obtenidos) y de rentabilizar los altos costes que implica todo este proceso de modernización[3].

Asimismo, y teniendo en cuenta nuestro complejo escenario competencial, dicha coordinación e interconexión también son indispensables para la propia viabilidad del nuevo sistema, pues es obvio que, si no se consigue, se seguirá operando como hasta ahora pero sustituyendo simplemente el papel por el soporte electrónico. Y es que debe recordarse que son precisamente las ventajas que ofrece el uso de las TIC en la gestión y transmisión de la información las que permiten que pueda tener lugar un nuevo modelo de funcionamiento, pues la intensificación de las relaciones internas y la disposición de un fondo de información común son la base de su revolucionaria eficacia, eficiencia y agilidad.

Administración electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant Lo Blanch).

2 Véase un estudio completo sobre la sede electrónica de la AEAT en Oliver Cuello, R. (2011). La sede electrónica de la Agencia Estatal de Administración Tributaria, pág. 44-54. *IDP. Revista de Internet, Derecho y Política* (12).

3 En la misma línea se pronuncia Sánchez, quien recalca, además, la necesidad de adoptar otras medidas específicas que reflejen nuestra complejidad institucional y que consoliden los tres niveles de Administración. (Sánchez Figueroa, J.C. (2006). Evaluación del nivel de desarrollo del gobierno digital en el ámbito autonómico y local (pág. 104). *CIE* (197)).

De igual modo, en tanto que el procedimiento de aplicación de los tributos se fundamenta en la interacción de la Administración con los ciudadanos, deben aprovecharse los nuevos recursos para simplificar al máximo la actuación de éstos (tanto para que puedan realizarla de forma correcta como para paliar las cargas derivadas de su colaboración), lo que sólo resulta posible si se aprovechan los beneficios que aporta la interconexión administrativa para eximirles de realizar actuaciones no estrictamente necesarias (como puede ser la presentación de unos mismos documentos a distintas Administraciones) y si se potencia la idea de una única Administración (facilitándose así, por ejemplo, la obtención de la información de la que precisen).

Además, si se prescinde de la misma, la incorporación de las TIC puede conllevar precisamente el efecto inverso a dicha simplificación, ya que la puesta a disposición de una multitud de canales, plataformas o sistemas que no se encuentran interconectados o la exigencia de diferentes certificados de usuario en cada Administración pueden llegar a constituir una auténtica barrera para la actuación de los administrados[4].

Así pues, el paradigma para la definitiva instauración de la e-Administración precisa de la actuación conjunta de todos los niveles administrativos, por lo que, sin dejar de seguir avanzando en la incorporación de las TIC de última generación en todas las Administraciones (especialmente en los servicios telefónicos, donde los índices de atención aún no son del todo suficientes), debe trabajarse para hacer de la coordinación, la cooperación, la compatibilidad técnica, la interoperabilidad y la creación de la denominada «ventanilla única» una realidad.

3. LA ADAPTACIÓN DE LA NORMATIVA TRIBUTARIA

Una vez realizada la importante inversión inicial en los nuevos medios y equipamientos, el segundo estadio imprescindible por el que debía pasar el proceso hacia la e-Administración debía ser la adaptación normativa, punto que realmente no era fácil teniendo en cuenta el desconocimiento generalizado de las TIC y el respeto a todas las garantías y exigencias que impone el Derecho administrativo tradicional. En especial, debía salvaguardarse la posición jurídica de los ciudadanos evitando cualquier menoscabo en función del medio utilizado, lo que requería tanto modificar las disposiciones ya existentes como crear la normativa necesaria.

Sin embargo, en relación con el ámbito propiamente administrativo, cierto es que el primer reconocimiento del uso potestativo de las TIC para el desarrollo de la actividad

4 En la misma línea, véase Cerrillo Martínez, A. (2008). Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica (pág. 498). En *Comentarios a la Ley de Administración electrónica. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*. Pamplona: Aranzadi.

administrativa (artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico del Procedimiento Administrativo Común –LRJPAC–) se ha convertido hoy en una ley de carácter básico en materia de Administración electrónica (Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos –LAECSP–), la cual ha aportado un marco jurídico completo sobre la misma y ha acabado con el carácter fragmentario y disperso de la normativa al respecto.

Además, ha creado un auténtico estatuto jurídico de los ciudadanos frente a la e-Administración, donde, si bien ha reiterado algunos de los derechos ya existentes y ha recalcado meras obviedades (básicamente con el fin de aumentar la confianza en los nuevos medios), ha incorporado algunos derechos inéditos derivados de las propias características de las nuevas tecnologías (como el derecho a elegir las aplicaciones o sistemas).

Asimismo, ha llegado a ampliar algunos de los derechos administrativos tradicionales (como ocurre en la extensión del derecho a la no aportación de documentos ya aportados a la Administración actuante a los aportados a cualquier Administración Pública), justificando su procedencia (es decir, la ausencia de discriminación de los ciudadanos que actúen a través de los medios tradicionales) con base en la imposibilidad de prestar dichas extensiones sin contar con las posibilidades que ofrece el uso de las TIC.

De todos modos, la mayor relevancia de este catálogo radica en el reconocimiento del derecho general de los ciudadanos a la utilización de la vía electrónica en sus relaciones administrativas, del cual deriva, por primera vez, la obligación de instaurar las TIC por parte de la Administración. Y, como acertadamente señala BAUZA, procede remarcar que dicha disposición no sólo es de índole tecnológica, sino que también debe concebirse desde el punto de vista físico o material. Por ello, y al margen de tener que disponer de los medios suficientes, la Administración también está obligada a poseer modelos normalizados de documentos electrónicos, y es que la «intensidad del tratamiento automatizado de la información en las Administraciones Públicas es tal, que una comunicación ordinaria al margen de una aplicación específica puede resultar no legible para la Administración»[5].

No obstante, cierto es que su carácter programático, la existencia de carencias e imprecisiones y el excesivo optimismo de algunas de sus disposiciones siguen dejando latente la necesidad de seguir avanzando en este campo, y más teniendo en cuenta que las TIC y, por ende, su inclusión se encuentran en constante evolución. Quizás por este motivo o por la falta de precedentes en la materia, todavía no se ha definido ni siquiera el concepto de «Administración electrónica», lo que supone una muestra más del gran trabajo normativo que aún falta por hacer.

Asimismo, idénticas consideraciones pueden aplicarse en relación con la normativa propiamente tributaria, aunque es de justicia destacar su carácter pionero en esta ma-

5 Bauzá Martorell, F.J. (2003). *Procedimiento administrativo electrónico* (págs. 52, 53 y 79). Granada: Comares.

teria y el extenso desarrollo que ha tenido. En este sentido, debe remarcarse que gran parte de las previsiones que la LAECSP ha hecho extensivas a todas las Administraciones Públicas (como el reconocimiento de las imágenes electrónicas o de la actuación administrativa automatizada) ya habían aparecido en el ámbito tributario con anterioridad, y es que, a pesar de la conveniencia de acabar con la previsión potestativa de la incorporación de las TIC en la esfera tributaria (artículo 96 de la LGT), ha sido la regulación que, a través de previsiones específicas en normas sobre procedimientos o tributos o a través de órdenes ministeriales *ad hoc,* ha servido de referencia tanto a nivel nacional como internacional.

De todos modos, conviene insistir en el carácter no estático de los nuevos medios y técnicas y su constante evolución, por lo que, sin desmerecer el gran desarrollo de la normativa tributaria en este punto, no puede dejar de seguir avanzando, buscando la excelencia y procurando el mejor y definitivo asentamiento de la e-Administración.

4. LA BÚSQUEDA DE LA PLENA INCLUSIÓN DIGITAL

Por último, en relación con esta lógica tercera fase, resulta evidente que la generalización de la utilización de las TIC en la ciudadanía constituye un presupuesto ineludible para la efectividad de la Administración electrónica, y más considerando que la desaparición del papel y la práctica exclusiva de relaciones electrónicas constituyen su ideal. Consecuentemente, una vez que se han cubierto las necesidades técnicas y normativas más relevantes, las Administraciones se han visto obligadas a paliar los efectos de la brecha digital, y más teniendo en cuenta que se ha convertido en uno de los intereses generales de la nueva sociedad.

Nuevamente, la actuación de la Administración tributaria ha sido un punto de referencia para el resto de Administraciones tanto españolas como internacionales, ya que, además de crear numerosas medidas específicas (como los Puntos de Acceso a Internet, los Puntos de Atención Ciudadana o el Centro de Atención Telefónica de Informática Tributaria), ha instaurado una multiplataforma de acceso electrónico e incluso ha establecido las primeras imposiciones del uso de las TIC en un trámite que afecta a la totalidad de obligados tributarios (como ocurre con la presentación de la declaración del Impuesto Especial sobre Determinados Medios de Transporte sobre operaciones sujetas y no exentas relativa al modelo 597). Obviamente, su exigencia supone el impulso definitivo para la generalización de su empleo, aunque debe acompañarse tal medida de los correspondientes recursos necesarios para evitar cualquier tipo de discriminación[6].

6 Véase un estudio sobre las principales medidas adoptadas por la Administración tributaria española para luchar contra la brecha digital en Rovira Ferrer, I. (2009). La inclusión digital en la Administración tributaria española (págs. 54-80), *Revista Técnica Tributaria* (86).

De todos modos, los datos más recientes demuestran la ineficacia general de todas las políticas públicas adoptadas al respecto, ya que, a pesar de que el número de usuarios de las TIC aumenta año tras año, aún no se ha logrado una cifra significativa entre los obligados tributarios. Así pues, sin dejar de velar por la mejora necesaria de las cuestiones técnicas y normativas, la inclusión digital debe seguir configurándose como el principal objetivo a abordar, pues a pesar de que los esfuerzos invertidos puedan ser calificados como más que satisfactorios, tanto la Administración tributaria electrónica como la sociedad de la información y el conocimiento aún no se encuentran asentadas de forma plena y definitiva.

5. UN NUEVO MODELO DE ADMINISTRACIÓN TRIBUTARIA

Obviamente, son muchas las consecuencias de la incorporación de las TIC en el seno de la Administración tributaria (desde un punto de vista de eficacia y eficiencia hasta una nueva forma de funcionamiento), y es que, sin ir más lejos el propio concepto de Administración electrónica entraña un nuevo significado de lo que debe ser esta tradicional institución.

Sin embargo, en el ámbito tributario, todo este proceso de tecnificación ha ido mucho más allá y ha comportado una nueva vuelta de tuerca en la propia configuración del modelo administrativo, convirtiendo así la Administración tributaria en un ente esencialmente asistencial.

Así, como bien es sabido, el tradicional sistema de aplicación de los tributos fijado por la LGT de 1963 se concebía como una sucesión de procedimientos separados entre sí que, siguiendo el esquema del proceso judicial, apostaba por una «aplicación artesanal» de los mismos[7].

En concreto, el procedimiento se iniciaba por la presentación de una declaración por parte de los sujetos pasivos o a consecuencia de una investigación administrativa, de modo que, una vez se conocía el hecho imponible, la Administración emitía una liquidación provisional. En ella se declaraba la existencia de una deuda tributaria, se determinaba su cuantía y se hacía exigible con su notificación, lo cual iniciaba la fase recaudación. Ésta concluía con el pago en período voluntario o tras la apertura de un procedimiento de apremio, lo que iba seguido de la oportuna inspección si se había presentado una declaración.

En ella se comprobaba la veracidad de los datos facilitados y se examinaba la existencia de hechos imponibles u otras circunstancias no manifestadas, después de lo que

7 Entre otros, así lo define Pérez Royo, F. (2002). *Derecho Financiero y Tributario. Parte General.* Madrid: Civitas, págs. 192 y 193.

actuaban nuevamente los órganos de gestión dictando una liquidación definitiva. En caso de no coincidir con la provisional, se notificaba nuevamente a los sujetos exigiéndoles el pago que debía proceder, lo cual, salvo incumplimiento o recurso, cerraba la aplicación de los tributos.

Sin embargo, este procedimiento liquidador sólo podía operar en un sistema tributario caracterizado por pocas actuaciones administrativas, de modo que, tras la aparición de impuestos de carácter masivo (especialmente del IRPF y el IS), su funcionamiento resultó totalmente impracticable. Como es lógico, la Administración no podía hacerse cargo de dictar un acto de liquidación provisional con la oportuna inspección en cada caso, y es que pasaron a existir millones y millones de deudas anuales por cada una de las más importantes figuras impositivas. Así pues, la incorporación de técnicas de gestión en masa se hizo totalmente necesaria, dentro de las cuales destacó especialmente la denominada autoliquidación.

A través de dicha figura, se concentró en un solo acto a cargo de los sujetos pasivos el deber de declarar, cuantificar e ingresar el hecho imponible sin necesidad de requerimiento previo, por lo que su actuación secundaria o auxiliar se convirtió en la más relevante del sistema de aplicación de tributos. Asimismo, la generalización de las autoliquidaciones comportó la reconfiguración de las labores administrativas, las cuales quedaron reducidas a las de comprobación e inspección. Sin embargo, a consecuencia de la relevancia de la actuación ciudadana, la comprobación debía verse potenciada, lo que condujo a la atribución de facultades al respecto a los órganos de gestión.

De igual modo, los órganos inspectores dejaron de practicar inspecciones en cada caso y, por razones de economía procedimental, se les otorgó competencia para practicar las liquidaciones resultantes de sus actuaciones de comprobación e inspección, lo cual supuso que la facultad para liquidar dejara de ser exclusiva de los órganos de gestión. A su vez, y como es lógico, quedó modificada la actuación de los órganos de recaudación, la cual quedó únicamente limitada a la fase de ejecución.

Así, y a consecuencia de la necesidad de controlar la actuación de los contribuyentes, se modificaron las funciones de todos los órganos del sistema, del mismo modo que se introdujo la actuación de terceros ajenos a la realización de hechos imponibles bajo la imposición de deberes de información y colaboración.

Como señala Soler Roch, el reconocimiento normativo de esta evolución puede situarse desde 1963 hasta, más o menos, 1986, período en el que se pasó de reconocer la existencia de las autoliquidaciones a introducirlas con carácter general[8]. En este sentido, el punto de partida se encuentra en la LGT de 1963, y es que, si bien les hizo caso omiso a la hora de regular el procedimiento de gestión tributario, su artículo10.*k*) exigió, por

8 Soler Roch, M.T. (1997). El sistema de gestión tributaria: problemas pendientes (pág. 50). En *Temas pendientes de Derecho Tributario.* Barcelona: Cedecs.

primera vez, el rango legal para su regulación. Seguidamente, no fue hasta 1965 que aparecieron las primeras manifestaciones en el sistema, las cuales se vieron aumentadas por la reforma tributaria de 1978 a consecuencia de la aprobación de la Constitución y del Real Decreto 357/1979 (que implantó el IRPF y el IS). Y, finalmente, su generalización tuvo lugar en 1986, donde las reformas previas de la LGT y la aprobación del Reglamento General de la Inspección de los Tributos sustituyeron el sistema tradicional de aplicación en la práctica totalidad de impuestos estatales por la implantación definitiva del régimen de autoliquidación. De este modo, la liquidación tradicional quedó reducida a los tributos de contraído previo, así como a los casos de autoliquidaciones irregulares o no realizadas.

Actualmente, las autoliquidaciones se encuentran principalmente reguladas en el artículo 120 de la LGT, donde se definen en su apartado 1 como las «declaraciones en las que los obligados tributarios, además de comunicar a la Administración los datos necesarios para la liquidación del tributo y otros de contenido informativo, realizan por sí mismos las operaciones de calificación y cuantificación necesarias para determinar e ingresar el importe de la deuda tributaria o, en su caso, determinar la cantidad que resulte a devolver o a compensar». Asimismo, el segundo apartado reconoce la posibilidad de que sean verificadas o comprobadas por parte de la Administración tributaria (quien, en su caso, practicará la liquidación que proceda), del mismo modo que el apartado 3 reconoce la posibilidad de instar su rectificación cuando los obligados tributarios consideren que les perjudican sus intereses legítimos (lo que se tramitará a través del procedimiento que se regule reglamentariamente).

Así pues, como señala Escribano, esta nueva forma de funcionamiento ha derivado en una actitud más pasiva de la Administración, la cual ha quedado básicamente reducida a controlar el cumplimiento de los deberes tributarios (comprobación e investigación) y a reaccionar ante su incumplimiento (procedimiento sancionador). De este modo, se pretende asegurar un nivel mínimo de recaudación y reducir, a su vez, los costes de funcionamiento, y es que son los obligados tributarios los que cargan ahora con la mayor parte de la actividad[9]. Sin embargo, esto conlleva que los ciudadanos deban conocer, interpretar y aplicar el complejo, cambiante e incluso, a veces, deficiente ordenamiento tributario, lo cual, como es lógico, genera una situación difícil de sustentar.

Esta problemática se ha visto recogida por la jurisprudencia en varias de sus sentencias, como ocurre en el fundamento tercero de la STS 2429/2002, de 4 de abril de 2002. Así, se pone de manifiesto «la inevitable complejidad de los sistemas tributarios modernos y la exigencia a los ciudadanos de obligaciones de hacer (sin perjuicio de las obligaciones de dar) en ocasiones dificultosas y superiores a la capacitación media que

9 Escribano López, F. (1996). El procedimiento tributario tras la reforma de la LGT (pág. 10). *Quincena Fiscal* (10).

en esta materia cabe suponer en aquellos», si bien, como añade, «los poderes públicos (y, en especial, la Agencia Estatal de la Administración Tributaria) han mostrado un empeño constante, en los últimos tiempos, de facilitar el cumplimiento de las obligaciones fiscales, no sólo a través de unos sistemas informáticos que han alcanzado las más altas cotas mundiales, sino en todo cuanto supone simplificación y ordenación del inevitable componente burocrático».

No obstante, esta labor de marcado carácter formal no ha resultado en absoluto suficiente, y es que, como se apuntaba, el principal problema reside en las imprecisiones, carencias y dificultades que caracterizan la normativa tributaria. Por ello, y sin dejar el control de la actuación ciudadana, la Administración tributaria debe acompañar dichas actuaciones de simplificación con una fuerte prestación de sus deberes de información y asistencia, los cuales deben ayudar a comprender y aplicar de forma correcta el ordenamiento jurídico en cada caso particular. Y es que dicha necesidad ya no sólo es exigible desde el punto de vista de la seguridad jurídica, sino que resulta imprescindible si se pretende mejorar la eficacia administrativa y dar viabilidad al sistema a través de su colaboración forzosa.

Además, como señalan Delgado y Oliver, «la Administración no puede trasladar al ciudadano, de quien reclama su colaboración, los riesgos inherentes de un marco jurídico cada vez más complejo»[10], del mismo modo que no puede olvidarse que así se desprende de la propia Constitución[11].

En igual sentido se pronunció el Informe de la Unidad Especial para el Estudio y Propuesta de Medidas para la Prevención y Corrección del Fraude, donde se señaló que «el desarrollo de sistemas eficientes de información y asistencia al contribuyente, exigidos por la complejidad del sistema tributario y la generalización de las autoliquidaciones, constituye, además de una exigencia de toda Administración Tributaria moderna, un punto de apoyo básico en la política preventiva del fraude fiscal, destinada al fomento del cumplimiento voluntario y con efectos añadidos en la eliminación de tensiones innecesarias en la relación con los ciudadanos»[12].

Del mismo modo, organismos tan relevantes como la OCDE o la propia Comisión Europea también se pronunciaron al respecto, tal y como puede observarse, respectiva-

10 Delgado García, A. M. y Oliver Cuello, R. (2004). *El deber de información y asistencia a los obligados tributarios* (pág. 18). Valencia: Tirant lo Blanch.

11 En este sentido, además del principio de seguridad jurídica que establece el artículo 9.3, el artículo 103.1 configura el servicio a los ciudadanos como la principal finalidad de la actividad administrativa, del mismo modo que establece la eficacia como uno de los principios fundamentales que la deben regir.

12 *Informe de la Unidad Especial para el Estudio y Propuesta de Medidas para la Prevención y Corrección del Fraude,* de julio de 1994, págs. 158 y ss.

mente, en el *Taxpayers' Rights and Obligations. A survey of the legal situation in OECD countries*[13] o en el *Informe sobre recaudación y control del IVA*[14].

Por ello, tal y como quedó reflejado en el Plan General de Objetivos de la AEAT para 1999, la Administración actuó en consecuencia y fijó como uno de sus grandes retos la intensificación de la prestación de los mencionados deberes en el cumplimiento voluntario de las obligaciones tributarias, lo cual, según se establecía, pretendía llevar a término a través de los siguientes medios: la potenciación de las vías de comunicación con el ciudadano que no conllevaran desplazamientos (como la atención telefónica e Internet), la incentivación de la comunicación previa de los datos relativos a los contribuyentes en relación con el IRPF que constan en la Base de Datos Nacional de la AEAT, el aumento de puntos de atención al ciudadano a efectos de la aplicación del programa PADRE y el fomento general de la cumplimentación y presentación de declaraciones tributarias por vía telemática.

Y quince años más tarde puede constatarse el gran el trabajo realizado y los buenos resultados obtenidos en cada uno de los objetivos citados, pues la AEAT ha dejado de centrarse en la instauración de nuevos servicios para pasar a fijar como gran reto el aumento de su mejora y calidad.

Por consiguiente, es justamente dicha gran labor general junto con las actuaciones de información y asistencia más importantes que se han implementado (la confección del borrador de declaración del IRPF, la posibilidad de que sea ella quien elabore las declaraciones de renta, la extensión de programas de ayuda y el aumento general de todos los servicios y trámites ofrecidos a través del portal virtual) el pilar que ha marcado un nuevo paso en el proceso evolutivo, es decir, el cambio importante y necesario hacia una Administración tributaria eminentemente asistencial.

Sin embargo, como señalan Delgado y Oliver, la Administración debería aprovechar todo su potencial de información y de herramientas informáticas y telemáticas que posee para mirar de centrar sus esfuerzos en la descarga generalizada de la que es, probablemente, la mayor obligación formal de los obligados tributarios: la determinación de la deuda tributaria, lo cual, en ningún caso, supondría un retroceso hacia el sistema de aplicación de tributos tradicional[15]. De todos modos, bien es cierto que la Administración tributaria ha procurado actuar al respecto, y es que, además de ofrecer la posibilidad de pedir cita previa para la realización de declaraciones de Renta, ha creado dos supuestos donde es ella la encargada de la cuantificación.

---

13 *Taxpayers' Rights and Obligations. A survey of the legal situation in OECD countries,* OCDE, París, 1990.

14 *Informe sobre recaudación y control del IVA,* Comisión Europea, 2004. (COM/2004/0855 final).

15 Delgado García, A. M. y Oliver Cuello, R.: *El deber de información y asistencia a los obligados tributarios*, cit., pág. 37.

Así, en un primer momento, el artículo 100 del Texto Refundido de la Ley del Impuesto sobre la Renta de las Personas Físicas, aprobado por el Real Decreto Ley 3/2004, de 5 de marzo, creó la denominada solicitud de devolución rápida, la cual ofrecía a determinados contribuyentes la posibilidad de dirigir una comunicación a la Administración tributaria para que determinara las cuotas pertinentes a los efectos del impuesto y procediera a su devolución. Sin embargo, y aunque preveía que la Administración pudiera requerir la presentación de la información y los documentos que resultaran necesarios, no se reconocía en ningún caso que la cuantificación del impuesto tuviera efectos de liquidación, lo cual no llegó hasta la posterior instauración del borrador de declaración por parte del artículo cuadragésimo segundo de la Ley 46/2002, de 18 de diciembre.

En este segundo caso, regulado actualmente por el artículo 98 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio (LIRPF), los contribuyentes obligados a presentar la declaración del IRPF pueden solicitar a la Administración tributaria que les remita un borrador de declaración a efectos meramente informativos, aunque, cuando el contribuyente considere que refleja su situación tributaria, podrá suscribirlo o confirmarlo y otorgarle efectos de declaración. Por el contrario, cuando el contribuyente considere que la información contenida no se ajusta a la real, podrá solicitar su modificación, o bien, como es lógico, presentar por su cuenta la correspondiente declaración. Así, gracias a la facilidad y rapidez de transmisión de las nuevas tecnologías y a las ventajas que permite el almacenamiento informatizado de los datos, la Administración ha sido capaz de dar un paso más, y ya no sólo por ofrecer la posibilidad de obtener una liquidación provisional a la práctica totalidad de contribuyentes obligados a declarar[16], sino también, y a

16 En este sentido, el artículo 98 de la LIRPF sólo prohíbe la solicitud del borrador a aquellos contribuyentes que no obtengan rentas procedentes exclusivamente de rendimientos del trabajo, de rendimientos del capital mobiliario sujetos a retención o ingreso a cuenta o derivados de Letras del Tesoro, de ganancias patrimoniales sometidas a retención o ingreso a cuenta, así como de subvenciones para la adquisición de vivienda habitual y de imputación de rentas inmobiliarias y de aquellas otras fuentes de renta que establezca el Ministro de Hacienda y Administraciones Públicas, de acuerdo con la información de la que pueda disponer en lo sucesivo la Administración tributaria, con los límites y condiciones señalados por el mismo. Asimismo, también lo impide en los casos donde se hubieran obtenido rentas exentas con progresividad en virtud de convenios para evitar la doble imposición suscritos por España, donde se tengan partidas negativas pendientes de compensar procedentes de ejercicios anteriores, en los casos que se pretenda regularizar situaciones tributarias procedentes de declaraciones anteriormente presentadas y cuando se tenga derecho a la deducción por doble imposición internacional y ejerciten tal derecho.

diferencia del caso anterior, porque los cálculos realizados por la misma son susceptibles de convertirse en una auténtica liquidación[17].

Viendo su gran acogida, su buen funcionamiento y sus notables ventajas, no es de extrañar que la idea de la Administración sea ir generalizando a todos los contribuyentes la utilización de esta figura, si bien sería también deseable que se extendiera su elaboración a los demás tributos existentes. Por contra, debe destacarse que, teniendo en cuenta el reducido número de contribuyentes que se acogían a la solicitud de devolución rápida, se optó finalmente por su desaparición a través de la Ley 35/2006, y es que realmente quedó obsoleta tras la generalización del borrador.

Así pues, la incorporación de la vía electrónica y esta clara tendencia hacia la potenciación de una mayor información y asistencia están suponiendo una gran evolución y mejora del sistema tributario en su conjunto, y es que no sólo se incrementa el ejercicio y la calidad de los mencionados deberes administrativos con la correspondiente disminución de la presión fiscal indirecta, sino que también se perfeccionan las funciones de control de la Administración. Al mismo tiempo, se incrementan las relaciones de colaboración entre las propias Administraciones y se favorece el desarrollo de los derechos y garantías de los contribuyentes, por lo que, en última instancia, se consigue un mayor acercamiento al ciudadano, una mejora en la calidad, eficacia y eficiencia de la actividad administrativa y una reducción general de todos sus costes y recursos. Y es que, en suma, como resumen Delgado y Oliver, las TIC han generado una Administración con mayor rendimiento, que cuesta menos y trabaja mejor[18].

Por ello, no es de extrañar que las ventajas que genera la utilización TIC en este campo compensen, y con creces, los esfuerzos y recursos invertidos, ya que, si bien es el ámbito donde se encuentra el mayor desarrollo normativo y material al respecto, también es donde se han registrado los mayores beneficios.

6. CONCLUSIONES

Como parte integrante de la misma, los cambios que ha ido experimentado la Administración Pública también se han visto reflejados en el seno de la Administra-

17 A diferencia de lo que ocurre en los casos donde la Administración elabora las liquidaciones de los contribuyentes con los datos aportados por los mismos, aquí se hace totalmente responsable de los datos que utiliza, de modo que, en caso de ser confirmados o suscritos, los contribuyentes no se encuentran con la carga de tener que probar los datos que facilitaron a la Agencia para probar el seguimiento de los criterios administrativos (lo cual, aparte de muy complicado, es prácticamente imposible de demostrar).

18 Delgado García, A. M. y Oliver Cuello, R. (2006). Principales aplicaciones de Internet en la Administración Tributaria (pág. 1). *IDP. Revista de Internet, Derecho y Política (2).*

ción tributaria, donde la figura del ciudadano y su colaboración se han convertido en piezas clave del sistema. Sin embargo, la introducción de las TIC en esta esfera ha dado un paso más y ha conllevado el nacimiento de un nuevo modelo de funcionamiento, en el que ha aparecido una Administración más abierta y comunicativa que, al facilitar más información sobre su funcionamiento y competencias, fomentar sus prestaciones y conseguir una mayor agilización de sus trámites y procedimientos, ha logrado un importante acercamiento al ciudadano y una mejora de su eficacia, calidad y rentabilidad.

Así, las nuevas actuaciones que han aparecido (especialmente la elaboración de declaraciones por parte de la Administración y la confección de borradores de declaración) han marcado el cambio de una Administración básicamente controladora a una Administración eminentemente asistencial, donde la presión fiscal indirecta se encuentra compensada más que nunca en tanto que la Administración vuelve a realizar gran parte de los deberes formales de los obligados tributarios.

En este sentido, las TIC han permitido que vuelva a ser la Administración quien elabore parte de las declaraciones de los obligados tributarios, aunque, lejos de suponer un retroceso hacia el procedimiento de aplicación de los tributos inicial, se ha iniciado un nuevo modelo de funcionamiento que sigue basado en las autoliquidaciones y deberes a cargo de estos últimos pero que avanza hacia conseguir un sistema de gestión compartida. Además, a pesar de que la mayor parte de la responsabilidad del sistema de aplicación de los tributos siga recayendo en exclusiva en los ciudadanos, la exoneración de responsabilidad por infracción tributaria derivada de actuaciones de información y asistencia y la posibilidad de reclamar la oportuna responsabilidad patrimonial administrativa por los daños y perjuicios que se puedan generar protegen, en gran medida, la posición jurídica de éstos, por lo que también puede afirmarse que, en cierto sentido, incluso se encuentra compartida la responsabilidad.

Sin embargo, debe destacarse en este punto que, a los efectos de potenciar aún más este nuevo modelo, resultaría más que conveniente la extensión de las principales actuaciones de asistencia mencionadas a todos los obligados tributarios, de la misma forma que, con base en sus múltiples beneficios, sería más que deseable preverlas en relación con todos los tributos (ya que actualmente se encuentran limitadas al ámbito del IRPF y se excluyen determinados sujetos de su recepción).

De todos modos, no debe olvidarse que, a pesar de los grandes esfuerzos invertidos en la tecnificación administrativa y en la adaptación de la regulación general (hasta el punto de convertirla en todo un referente), la Administración tributaria debe seguir velando por incorporar las tecnologías más avanzadas y por perfeccionar la normativa existente, de la misma forma que, al margen de maximizar los recursos en la lucha contra la brecha digital, debe centrarse en lograr un avance conjunto y coordinado para conseguir la máxima homogenización y la plena interconexión e interoperabilidad.

7. BIBLIOGRAFÍA

Bauzá Martorell, F.J. (2003). *Procedimiento administrativo electrónico*. Granada: Comares.

Cerrillo Martínez, A. (2008). Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica. En *Comentarios a la Ley de Administración electrónica. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*. Pamplona: Aranzadi.

Cerrillo Martínez, A. (2010). La difusión de información pública a través de medios electrónicos: claroscuros de la Ley de acceso electrónico de los ciudadanos a los servicios públicos. En *Administración electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y los retos jurídicos del e-gobierno en España.* Valencia: Tirant Lo Blanch.

Delgado García, A.M. y Oliver Cuello, R. (2006). Administración tributaria electrónica y software libre (págs. 22 y 23). *Revista de Información Fiscal* (75).

Delgado García, A.M. y Oliver Cuello, R. (2006). Principales aplicaciones de Internet en la Administración Tributaria. *IDP. Revista de Internet, Derecho y Política (2).*

Delgado García, A.M. y Oliver Cuello, R. (2004). *El deber de información y asistencia a los obligados tributarios*. Valencia: Tirant lo Blanch.

Escribano López, F. (1996). El procedimiento tributario tras la reforma de la LGT, *Quincena Fiscal* (10).

Mas, O.; Palomo, L.; Carreras, R.; Fabra, E. y Genové, F. (2004). El «software» libre, el último tren de la emancipación tecnológica. *Coneixement i Societat, Revista d'Universitats, Recerca i Societat de la Informació* (5).

Oliver Cuello, R. (2011). La sede electrónica de la Agencia Estatal de Administración Tributaria. *IDP. Revista de Internet, Derecho y Política (12).*

Pérez Royo, F. (2002). *Derecho Financiero y Tributario. Parte General.* Madrid: Civitas.

Rovira Ferrer, I. (2009). La inclusión digital en la Administración tributaria española, *Revista Técnica Tributaria* (86).

Sánchez Figueroa, J.C. (2006). Evaluación del nivel de desarrollo del gobierno digital en el ámbito autonómico y local. *CIE* (197)

Soler Roch, M.T. (1997). El sistema de gestión tributaria: problemas pendientes. En *Temas pendientes de Derecho Tributario*, Barcelona: Cedecs.

SOBRE LA SIMPLIFICACIÓN ADMINISTRATIVA Y LA PERVERSIÓN DE LAS SOLICITUDES GENERADAS ELECTRÓNICAMENTE QUE NEUTRALIZAN LA REDUCCIÓN DE CARGAS ADMINISTRATIVAS

Mª Dolores Rego Blanco
Profesora Titular de Derecho Administrativo
Universidad Pablo de Olavide

RESUMEN: El tema de esta comunicación se aborda desde la perspectiva jurídica y se sitúa en la intersección de dos ejes de la modernización de la Administración Pública, como son la Administración electrónica y la simplificación administrativa (en concreto, en el objetivo político y jurídico de la reducción de cargas administrativas).

En la actualidad, la preocupación por ajustar las cargas administrativas a lo imprescindible, de manera que las empresas, y los ciudadanos en general, no hayan de dedicar más dinero ni tiempo que el estrictamente necesario para cumplir con las exigencias legales, se refleja como mandato en textos legales. Puesto que uno de los factores determinantes de la minoración de cargas administrativas es el tiempo necesario para atender los requisitos legales, se ha asentado como premisa incuestionada la relación positiva entre implantación de la administración electrónica y la reducción de costes burocráticos.

La comunicación cuestiona esta relación y pone de manifiesto las disfunciones que pueden provocarse si los sistemas normalizados de solicitud que hay que emplear para iniciar procedimientos administrativos se diseñan sin las suficientes cautelas, pues, a parte de exigir un aumento de tiempo nada despreciable en la presentación de solicitudes, ponen en riesgo la integridad de garantías jurídicas de los ciudadanos ante las Administraciones Públicas. Como conclusión se apunta a la necesidad de que la Administración asuma su carácter servicial (art. 103 CE) y evite que la implementación de los procedimientos administrativos que ella protagoniza evite toda neutralice la reducción de cargas administrativas.

PALABRAS CLAVE: Modernización de la Administración Pública. Simplificación administrativa. Administración electrónica. Cargas administrativas. Modelos normalizados de solicitud. Sistemas normalizados de solicitud. Derechos de los Ciudadanos.

1. INTRODUCCIÓN

En el marco de las políticas de modernización de las Administraciones Públicas y de mejora regulatoria, y persiguiendo el objetivo de la simplificación de los procedimientos administrativos, la necesidad de reducir cargas administrativas se ha asumido tanto en Programas y Acuerdos gubernamentales, como en normas jurídicas, donde se consagra

con carácter principial y programático[1]. Muy sintéticamente expresado, el fin último del empeño en la eliminación de cargas administrativas es evitar que haya recursos económicos que se destinen baldíamente a cumplir con obligaciones formales innecesarias, injustificadas o desproporcionadas, y así maximizar los recursos económicos del sistema que pueden aplicarse a otros fines beneficiosos para la Sociedad; simultáneamente, me gusta añadir, se maximiza el contenido de la libertad humana, en justo equilibrio con las limitaciones a que obliga su encaje con el interés público.

2. POR QUÉ CON LA IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA SE PUEDEN REDUCIR LAS CARGAS ADMINISTRATIVAS

Pese a haberse juridificado, el concepto de carga administrativa aún carece de definición legal (al menos de carácter básico[2]) y eso propicia que pueda pensarse que las normas que propugnan la simplificación administrativa mediante la reducción de cargas no se están refiriendo a ninguna realidad concreta y distinta del ahorro de requisitos administrativos o de limitaciones de derechos. Es muy frecuente encontrar esta confusión en textos normativos[3], y también entre la doctrina, que expone su prevención a que la reducción de cargas administrativas pueda perjudicar la salvaguarda de intereses públicos[4].

Para entender por qué la administración electrónica es instrumento ideal para eliminar cargas administrativas es preciso afianzar el concepto de «cargas administrativas»: son cantidades de dinero, no requisitos legales. Representan un subconjunto del dinero que se dedica a cumplir con las exigencias que el ordenamiento jurídico impone. Son la

1 *Vgr*. acuerdo de Consejo de Ministros de 4 de mayo de 2007 (BOE de 12.6); o, acuerdo de la Junta de Castilla y León 22/2014, de 30 de enero, (BOCYL de 3.02); y el art. 4 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

2 La Ley castellano-leonesa 5/2013, de 19 de junio las define como «aquellas informaciones obsoletas o innecesarias que las empresas tienen que aportar a la administración como consecuencia de su funcionamiento y su diligente gestión» (art. 8).

3 Véase la nota anterior, donde se hace equivaler a «información»; o la utilización del término en la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado, que nunca deslinda del concepto «requisito legal»; o en la Orden de 12 de enero de 2012 por la que se regula la habilitación de procedimientos administrativos y servicios, de Galicia, donde se define como actividades de naturaleza administrativa que deben llevar a cabo las empresas y los ciudadanos para cumplir con las obligaciones derivadas de las normas reguladoras de procedimientos administrativos o servicios y que no harían de no venir impuestos por éstas».

4 Así, GAMERO CASADO o DOMÉNECH PASCUAL en sus ponencias en el IX Congreso Nacional de la Asociación Española de Derecho Administrativo, (http://www.aepda.es/EscaparateFamilia.aspx?id=71-Actividades-Congresos-de-la-AEPDA.aspx respectivamente p. 57 y 25)

parte de los costes derivados de la legislación, en que se incurre por realizar actividades administrativas formales por la directa y exclusiva imposición de la regulación, de modo que, de no existir ésta, no habría que soportarlos[5]. Son costes de gestión burocrática o formal (costes de «papeleo, si se quiere), no de cumplimiento sustantivo de requisitos jurídicos (costes de cumplimiento).

La cuantificación de la carga administrativa se hace con carácter estimativo, a través de la fórmula[6]:

CARGA ADMINISTRATIVA = precio × tiempo × cantidad,

(todo en referencia a la actividad burocrática formal derivada de requisitos sustantivos)

En la ecuación, el factor «precio» alude a los costes salariales y gastos generales generados en el desarrollo de la actividad administrativa en el seno interno de la organización de la empresa. El factor «tiempo» refleja la cantidad de tiempo necesario para realizar la actividad administrativa[7]; y finalmente, el factor «cantidad» resulta de multiplicar la población afectada (o número de empresas que deben realizar la actividad administrativa) por la frecuencia con que la actividad administrativa ha de llevarse a cabo. Así, si una actividad administrativa tarda 3 horas en completarse (tiempo) y el coste/hora del trabajador que la está realizando es de 10 euros (tarifa), cada empresa aplicaría 30 euros en realizarla. Si el requisito se aplica a 100.000 empresas (población) y cada una tuviese que cumplirlo 2 veces al año (frecuencia), la carga administrativa se elevaría a 6.000.000 euros.

A través de esta fórmula queda patente que los costes representados por las cargas administrativas no solo se reducen eliminando requisitos jurídicos sustantivos de los que deriva la necesidad de realizar la actividad administrativa o burocrática (cuyo coste se expresa como carga administrativa). Aún manteniendo requisitos jurídicos, las cargas administrativas pueden aliviarse incidiendo en los factores que integran la fórmula básí-

5 Consúltese *International Standard Cost Model Manual, Meausring and reducing administrative burdens for businesses,* accesible en http://www.administrative-burdens.com (visitada en 06/06/2013), y REGO BLANCO (2014: p 244 y ss). Interesa aclarar que las cargas administrativas, en cuanto costes económicos, no son: a) ni el dinero de pagar tributos por realizar la actividades económicas; b) ni el que, en términos de oportunidad o de competitividad, y a largo plazo, comporta una determinada regulación; c) ni aquéllos en se incurre para dar cumplir obligaciones sustantivas que impone la regulación; d) ni los costes de administración, derivados de la gestión interna de la empresa.

6 Es la fórmula del *Standard Cost Model*. Véase *ibídem*.

7 En España las Administraciones Públicas han consensuado un Método Simplificado de Medición de Cargas Administrativas y de su Reducción, que denomina coste unitario al producto del precio x dinero, asociándose de esta forma un coste único por tipo de trámite/carga acordado con las CCAA y la FEMP.

ca para su cálculo, de manera que el resultado del producto sea inferior. Precisamente así es como la implantación de la administración electrónica se ha ganado un incuestionado reconocimiento como mecanismo con gran potencial de reducción de cargas administrativas, y se ha propugnado por cualquier informe[8], plan o método de simplificación administrativa que se precie. Por ejemplo, si en lugar de tener que aportar fotocopia del DNI junto a una solicitud, basta con incluir la autorización a la Administración para que ella, gracias a las nuevas tecnologías, pueda verificar el dato, no se elimina el requisito jurídico de que el solicitante se identifique con un DNI, pero hacerlo será más barato para él, al ahorrarse el tiempo de preparar la fotocopia y el coste de la misma.

3. CÓMO PUEDE NEUTRALIZAR LA REDUCCIÓN DE CARGAS ADMINISTRATIVAS LA IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA

En el desarrollo de la política de reducción de cargas el protagonismo lo ha acaparado la fase de elaboración de las normas jurídicas, ya que las cargas administrativas están asociadas primordialmente al cumplimiento de los requisitos sustantivos diseñados normativamente para el ejercicio de cualquier derecho o deber. De este modo, los aspectos procedimentales de cómo simplificar cargas administrativas se han plasmado en la «evaluación de impacto normativo», comprensivo del correspondiente «estudio de cargas administrativas»[9], que actualmente es preceptivo en el procedimiento de elaboración de normas jurídicas[10]. En fase normativa lo que puede hacerse es revisar lo adecuado de los requisitos jurídicos exigidos y la forma burocrática de satisfacerlos (electrónica o no).

Sin embargo, no toda carga administrativa tiene su origen directamente en la norma jurídica sectorial. También puede generarse en la fase su ejecución, por lo que ésta no puede descuidarse. En este sentido, se ha apuntado a que el ejercicio de potestades discrecionales desconociendo el principio de intervención mínima (art. 39.1 bis Ley 30/1992) puede incrementar la carga administrativa, o también las exigencias de los empleados públicos que no guarden relación razonable con el objetivo perse-

8 Por todos, el reciente y conocido *Informe CORA*.

9 Sobre el particular puede interesar la consulta de BETANCOR (2009), CANALS (2010) o MORA RUIZ (2014).

10 Real Decreto 1083/2009, de 3 de julio, por el que se regula la memoria del análisis de impacto normativo; Ley foral 15/2009, de 9 de diciembre; o Decreto 48/2009, de 28 de abril (C.A. canaria) por el que se establecen en la Administración Pública de la Comunidad Autónoma de Canarias medidas ante la crisis económica y de simplificación administrativa; Decreto106/2008, de 6 de mayo (C.A. catalana), o Ley 6/2006, de 24 de octubre (C.A. andaluza), entre otros.

guido (como previene el Código de Buena Conducta Administrativa del Parlamento Europeo)[11].

Esta comunicación desea poner de relieve la importancia de cuidar la implantación de la Administración electrónica para una efectiva reducción de cargas administrativas. Para ello se va a analizar el trámite de iniciación del procedimiento mediante solicitud cursada con nuevas tecnologías. El coste estimado de cumplimentar y presentar de una solicitud se fija en 80 euros/unidad si es en papel y en 5 euros/unidad si es electrónica[12]. Esto es una mera estimación, no una verdad universal o indiscutible. La terca realidad puede ser muy otra puesto que existen muchos factores extra-jurídicos que pueden incidir en que, por un diseño inadecuado de los formularios integrados en sistemas normalizados de solicitud, se malogre la relación entre iniciación electrónica del procedimiento y reducción de cargas, frustrando el objetivo de simplificación a favor del ciudadano[13] y minorando sus garantías jurídicas. A continuación se recogen algunos de estos factores, ilustrándolos con algunos ejemplos extraídos del modelo de solicitud de evaluación de la actividad investigadora (sede electrónica de Educación del Ministerio), que está integrado en un sistema normalizado de solicitud. Seguramente que el lector pueda dar cuenta de algunos otros.

4. DISFUNCIONES DE LAS SOLICITUDES GENERADAS ELECTRÓNICAMENTE QUE PERJUDICAN LA SIMPLIFICACIÓN DE CARGAS ADMINISTRATIVAS

A la par que se avanza en la implantación de la Administración electrónica se incrementa el número de solicitudes que se preparan haciendo uso de las nuevas tecnologías. No hace falta recurrir a estudios[14] para constatar el enorme potencial de minoración de carga administrativa que ello supone; basta pensar en el ahorro de dinero y tiempo conseguido por no desplazarse a oficinas administrativas para conseguir los formularios oficiales; por tener los formularios disponibles sin limitaciones de horarios; por

11 REGO BLANCO (2014: p. 277 y ss).

12 Las tablas de costes estimados se extraen del documento *Método Simplificado de Medición de Cargas Administrativas y de su Reducción* (2009).

13 Forzado a incrementar de forma significativa el tiempo necesario para cumplimentar la solicitud electrónica, tiempo que no dedica a su actividad principal (que en un Estado de Derecho no puede ser atender a la burocracia, salvo que libremente se dedique profesionalmente a prestar servicios de gestoría)

14 Como el realizado por la Cámaras de Comercio y el Ministerio de Política Territorial y Administraciones Públicas en 2011, disponible en http://www.camaras.org/publicado/estudios/simplificacion_adm/publicaciones/impacto_reduc_cargas_re_def.pdf (consultado el 10 de marzo de 2014).

no tener, eventualmente, que repetir la cumplimentación completa de formularios por haber cometido errores; por evitar la presentación por multiplicado[15]; o, por no tener que ajustare al horario de atención al público del registro para realizar la presentación presencialmente.

Por otro lado, la aplicación de las nuevas tecnologías a las solicitudes a la Administración permite simultáneamente facilitar la gestión electrónica del expediente a que la solicitud de lugar y agilizar los procedimientos de tratamiento de los datos aportados en ellas para posteriores usos, con el consiguiente avance en eficacia y eficiencia administrativas (art. 103 CE) y ahorros de costes de trabajo para la Administración.

En lo delicado de la tarea de armonizar en la práctica los intereses de minimizar carga administrativa (para el ciudadano) y carga de trabajo (para la Administración) a través de las solicitudes generadas electrónicamente puede encontrarse la razón de que esta técnica de simplificación pueda provocar disfunciones que neutralicen la esperada reducción de carga administrativa.

Sin entrar en los problemas de accesibilidad de las sedes electrónicas[16], ni el interesante debate de cuál sea el límite para obligar a usar sistemas normalizados de solicitud o para que al requerir datos en sus formularios la Administración no esté trasladando al ciudadano la carga de trabajo que le corresponde asumir a ella[17] (y generándole, por tanto, carga administrativa), podemos aislar algunas de las maneras en que las solicitudes generadas electrónicamente requieren una mayor inversión de tiempo de cumplimentación y originan un incremento de la carga administrativa teóricamente reducida con su implantación. En concreto, propongo una reflexión sobre las siguientes:

---

15 La multiplicación puede ser por dos, por tres, o incluso más. Por sextuplicado se exigía la presentación de solicitud de evaluación de sexenios, como puede verse en la Resolución de 6 de febrero de 1990 de la Secretaría de Estado de Universidades e Investigación (BOE del día 8).

16 En relación con las restricciones admisibles por el art.35 Ley 11/2007.

17 Téngase en cuenta que el derecho reconocido en el art. 35. f Ley 30/1992 se refiere a la presentación de «documentos ( ) que ya se encuentren en poder de la Administración actuante», lo que no cubre un eventual derecho a no aportar en las solicitudes datos que ya tenga la Administración, y en definitiva, frente a la «Administración no electrónica» el ciudadano no tiene garantizado positivamente el no tener dedicar su actividad a volcar datos en los formularios, preparando su propio expediente como si él mismo fuera «personal administrativo». Sin embargo, frente a la Administración electrónica, sí que existe una previsión legal al respecto, pues el art. 6.2.b) de la Ley 11/2007 recoge el derecho de los ciudadanos «A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.»

4.1. La inclusión de «campos llave»

Con *campos llave* me refiero a aquéllos campos de solicitudes generadas electrónicamente que secuencian la introducción de datos porque, de no completarse o de no hacerse oportunamente, impiden que el usuario acceda al resto del formulario de solicitud, o que avance en la cumplimentación de otros datos, o incluso, los guarde.

Si el solicitante encuentra una dificultad al cumplimentar un *campo llave* del formulario del sistema normalizado de solicitud, el sistema no le permitirá que acceda al resto del formulario y continúe introduciendo otros datos que sí conoce; le forzará a tener que resolver su[18] problema para poder seguir con la solicitud. En ocasiones este factor de incremento de cargas se une a otros que veremos más adelante (como la deficiente rotulación de los campos), propiciando que el usuario incurra en reiterados errores, o más bien, «des-aciertos» a la hora de rellenar el campo, que aumentan su carga administrativa.

Aunque se proporcionen servicios de consulta telefónica o telemática, como mecanismos complementarios del alivio de cargas, la atención que brindan no siempre es inmediata (líneas sobrecargadas o que comunican; lapsos de días entre que se formula la solicitud y se recibe la contestación), ni suficientemente personalizada (respuestas estandardizadas), ni completa (no atiende aspectos sustantivos, sino meramente informáticos, sin que se consideren tales los relativos a qué información debe introducirse en el campo en cuestión o cómo plasmarla).

Como quiera que sea, puestos a ahorrar costes en la preparación de solicitudes electrónicas, no encuentro ventaja alguna en los *campos llave* porque impiden tener una visión completa de la solicitud o seleccionar la parte con la que se quiere trabajar. Me parece irrefutable que se invierte menos tiempo, dinero y energía vital si el formulario puede verse de principio a fin, puesto que pueden identificarse todos los problemas que requieran mayor atención, y plasmar en una única consulta todas las cuestiones necesarias para preparar la solicitud. Piénsese que secuenciar la navegación por el formulario en distintas etapas y condicionar el avance de una a otra a que los datos sean formalmente correctos, obligará a realizar distintas consultas y en diferentes momentos, y el usuario tendrá que emplear más tiempo en poder solucionar los problemas estrictamente burocráticos que le plantea la preparación de la solicitud (paralizará la preparación y requerirá ayuda del servicio de atención en tantas ocasiones como veces quede atrapado por un *campo llave*), con el riesgo, por otra parte, de coadyuvar a la sobresaturación del servicio de atención.

18 La cursiva enfatiza el que la Administración rara vez reconoce que estas situaciones las provoca ella misma con un deficiente diseño del formulario.

4.2. La normalización de los datos que el usuario debe aportar en los campos obligatorios, sin ofrecer un elenco tasado de opciones de respuestas

Una importante fuente de ahorro y simplificación del tratamiento de datos que corresponde hacer a la Administración para gestionar procedimientos consiste en aprovechar, gracias a las nuevas tecnologías, la actividad de introducción de datos que realiza el interesado en su solicitud. La Administración maximiza este ahorro si además de no tener que teclear los datos que proporcionan los usuarios, los datos se reciben normalizados con expresiones tasadas o con códigos predeterminados, de manera que su recogida, tratamiento y almacenamiento pueda realizarse automatizadamente[19].

Así, por ejemplo, en el sistema normalizado de solicitud de evaluación de sexenios de investigación, para evitar que el campo «Universidad de pertenencia» pueda recibir respuestas tan variadas en la forma como «U. Pablo de O.», «Univ. Pablo de Olavide», «Pablo Olavide» o «UPO», el sistema normalizado de solicitud puede dar como válida una única respuesta: «2186-UNIVERSIDAD PABLO DE OLAVIDE».

Pero esta opción, en principio legítima para la Administración, puede volverse en contra del administrado y ser fuente de un incremento de carga administrativa, como ocurre si en lugar de permitir que, de una manera u otra (mediante ventanilla desplegable; mediante anexos en las instrucciones de ayuda, etc.) el usuario conozca las distintas expresiones que admite el sistema para rellenar el dato, se le somete a un sistema de búsqueda, que, por lo poco inteligente, más se parece a un juego de adivinanza que a cualquier otra cosa. Siguiendo con el ejemplo anterior, hay un campo para el «cuerpo» al que pertenece el solicitante, y se configura como un *campo tipo buscador*, que es la denominación que se da al tipo de campo en donde el usuario, en lugar de introducir directamente el dato, debe teclearlo y pulsar en «buscar», para que el sistema informático le ofrezca ese mismo dato en el formato normalizado que debe incluir. Si en el ejemplo se introduce la denominación oficial del cuerpo, «catedráticos de universidad»[20], sorprendentemente el sistema responde «no existen registros que cumplan las condiciones de búsqueda». Se prueba con «catedra» y el programa ofrece dos respuestas válidas «0505 CATEDRATICO DE ESCUELA UNIVERSITARIA» Y «0500 CATEDRATICO DE UNIVERSIDAD». El sistema lo quiere en singular, y no es capaz, sólo por una letra, de identificar un registro similar.

---

19 Como destaca oportunamente VALERO (2007: 97).

20 Según el art. 56.1.a Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, o la propia convocatoria aprobada por Resolución de 21 de noviembre de 2013 por la Secretaría de Estado de Educación, Formación Profesional y Universidades (BOE de 2 de diciembre) que establece como requisito la pertenencia a alguno de los cuerpos docentes universitarios, entre ellos, el de «Catedráticos de Universidad» (en plural).

En el modelo de solicitud que nos sirve aquí de ejemplo, también es un *campo tipo buscador* el preparado para indicar la «Universidad/CSIC» de pertenencia. Probando con «Pablo de Olavide» el buscador ofrecía dos soluciones diferentes, con código de normalización distinto: el «2186#UNIVERSIDAD PABLO DE OLAVIDE» y el «56#UNIVERSIDAD PABLO DE OLAVIDE». Según las instrucciones (pág 5) «Algunos de estos campos [*tipo buscador*] están relacionados entre sí». Pero no especifican las instrucciones cuáles sí lo están y cuáles no. El resultado: el usuario tiene que decidirse por uno de los códigos sin saber las consecuencias de una u otra opción y si le condicionará en algún sentido (sustantivo o formal) su solicitud. Este tipo de situaciones generan incertidumbre en el usuario, cuando precisamente la creación de certidumbre es una de los medios generalmente proclamado como propio de la reducción de cargas administrativas[21].

Peor suerte se corrió con el campo obligatorio *tipo buscador* «Facultad o esc univ./centro», pues siendo la de pertenencia la Facultad de Derecho, el buscador no ofrecía «registros satisfactorios» ni proponiendo «facultad de derecho», ni «derecho», ni «facultad». Ignoro cómo logró salir de este aprieto el compañero que al pedirme ayuda en la última convocatoria para afrontar su solicitud, me suscitó la idea de preparar esta comunicación, pero doy fe de que le hizo emplear considerablemente más tiempo (y afrontar más carga) que si el formulario hubiera sido en papel; he consultado mi solicitud, que data de 2012, y en este campo figura «2186#UNIVERSIDAD PABLO DE OLAVIDE» ¿para qué pide el formulario un campo obligatorio específico sobre la Facultad? He aquí una pista de un nuevo factor de incremento de cargas administrativas a través de las solicitudes generadas electrónicamente, que merece un apartado propio.

Pero antes de continuar, es oportuno advertir que el mecanismo desarrollado como *campo tipo buscador*, a través del cual puede rechazarse la aportación de la información por la manera en que ésta se exprese (básicamente, por no coincidir con ninguna de las «expresiones tipo» que maneja el sistema) no puede considerarse, bajo ningún concepto, una «comprobación automática» de las que ampara el art. 35 LAE. La comprobación automática de datos admitida legalmente es una verificación de carácter sustantivo (no formal, como la que hace el *campo tipo buscador*) por cotejo con los datos que obran en poder de la Administración. Además, si la Administración estuviera en poder de dichos datos, lo que procedería sería, por un lado, que ella ofreciera la solicitud cumplimentada en los campos correspondientes a los datos en cuestión[22], para respetar el derecho del

21 REGO BLANCO (2014: p. 271).

22 En nuestro ejemplo, cuando el solicitante es funcionario de Cuerpos Docentes o funcionario de Cuerpos de la Administración del Estado, casi todos los datos administrativos del solicitante que requiere el formulario (Universidad, cuerpo, titulación, fecha de toma de posesión, etc.) son conocidos por la Administración convocante (que es la estatal) gracias al Registro central de personal.

ciudadano[23] a no tener que aportarlos (art. 6.2.a LAE); y por otro lado, adicionalmente, procedería que la Administración no enervase el derecho de los ciudadanos a corregir o completar tales datos, lo que puede obstaculizarse si el sistema introduce en el formulario *campos tipo buscador*, como los aquí analizados.

4.3. La introducción de campos obligatorios que no se corresponden con ninguno de los requisitos sustantivos de la solicitud, de acuerdo con su regulación

Jurídicamente no es de recibo que la Administración aproveche la necesidad de cursar una solicitud para obligar a suministrar informaciones que no guarden relación con los requisitos sustantivos (arts. 70 y 71 Ley 30/1992). Esto es así con independencia del tipo de solicitud que sea, pero en las solicitudes integradas en sistemas normalizados plantea mayor problema puesto que estos sistemas pueden reforzar la obligatoriedad de aportar esa información legalmente no exigible. Basta con asociar, como de hecho asocian, trabas a los campos identificados como obligatorios, de manera que si no se suministra la información (legalmente no exigible, insístase) se impida que se pueda continuar navegando por el formulario, o se impida generar la solicitud si el formulario si no está completo, etc.

Volviendo al caso propuesto como ejemplo, uno de los campos obligatorios era el de «Facultad o esc univ./centro», pese a que ninguna repercusión tiene sobre los requisitos sustantivos previstos por su régimen jurídico[24].

Evidentemente, si se establecen como obligatorios campos que no guardan relación alguna con los requisitos sustantivos de la solicitud, el resultado práctico va a ser, como mínimo, un aumento injustificado de la carga administrativa asociada a la preparación del escrito (menor o mayor según el campo se configure como «campo llave» o «campo tipo buscador no inteligente»), pero además, veremos que puede perjudicar la integridad de garantías jurídicas cuando el carácter obligatorio del campo supone que, pese a ser innecesario, si no se completa no se puede confirmar o generar la solicitud ni puede presentarse por registro.

---

23 No procedería la objeción de que por el hecho de que el solicitante sea empleado de la Administración no han de tenerse en cuenta los derechos de los ciudadanos. Aparte de que quien solicita lo hace a título personal, más como ciudadano que como empleado (puesto que con la solicitud no está ejerciendo ninguna función pública ni prestando servicio público alguno), hay que tener en cuenta que perjudica igualmente a la Administración obligar a su personal a emplear más tiempo del necesario en cumplimentar sus solicitudes.

24 Establecido por el Real Decreto 989/1986, de 23 de mayo, sobre retribuciones del profesorado universitario.

4.4. Rotular con ambigüedad los campos de la solicitud

Otro factor que puede desvanecer la reducción de carga administrativa es que los campos que ofrece el sistema normalizado de solicitud no estén suficientemente claros o bien identificados. Si son ambiguos puede tenerse que invertir más tiempo a la hora introducir el dato requerido, especialmente cuando el campo es del «tipo buscador» o tiene asociado un mecanismo de verificación por relación a otros campos.

Una vez más el modelo de solicitud de sexenios nos sirve para ilustrar este factor de aumento de cargas administrativas. Entre los datos personales, después de los imprescindibles «DNI», «apellidos» y «nombre», el sistema normalizado de solicitud pregunta por (éste orden) la «fecha de nacimiento», «sexo» y «país». Inmediatamente después sitúa el campo «Comunidad Autónoma» y luego los datos de la dirección postal, etc. Todos los mencionados son obligatorios en este formulario. Conozco quien, habiendo nacido en el extranjero, después de rellenar su fecha de nacimiento y su sexo, consideró que el campo «país» debía relacionarlo con «país de nacimiento», en lugar de país de residencia. Como ese campo esta informáticamente relacionado con el de «Comunidad Autónoma», cuando intentaba seleccionar la suya, el sistema informaba de la existencia del error, pero no aportaba dato alguno para deducir dónde estaba el error. Por supuesto, ni dejaba guardar los datos ya introducidos ni tampoco navegar hacia páginas ulteriores del formulario. ¿Qué trabajo cuesta que el formulario rotule con exactitud el campo país, añadiendo «de residencia»? Muy poco. ¿Cuánto tiempo de más supone para el usuario? Pues en este caso real, consumido el tiempo que ese día disponía para ocuparse de la solicitud, nuestro protagonista decidió dejarlo para el día siguiente, y probar a que le atendiera el servicio telefónico de asistencia. Lo que no se tardaba ni un minuto en rellenar, requirió un día más de pendencia.

Otro ejemplo de indeterminación en el mismo formulario: entre los datos administrativos del solicitante, el sistema normalizado incluye como campo obligatorio y con buscador uno rotulado «tipo de titulación». La ambigüedad viene aquí provocada porque la tipología de titulaciones es tan variada como criterios de clasificación se puedan idear. Puestos a probar, todos los intentos terminaban en «error». También en este caso real, se dejó pendiente la solicitud para otro día e incluso se tuvo que hacer uso del servicio de consultas pues el solicitante no acertaba a adivinar cómo expresar el dato (las instrucciones oficiales ilustraban este campo con la respuesta «especialista» …¿qué solicitante no lo sería?!). Es un caso llamativo porque, en mi opinión, el dato es prescindible, por no corresponderse con ningún requisito sustantivo. Como pese a ello, el sistema lo tiene por obligatorio, la mejorable rotulación del campo termina forzando a emplear más tiempo del necesario en la preparación de la solicitud, e incluso a utilizar el servicio de consultas, generando tanto carga administrativa para el usuario como carga de trabajo para la Administración (la de atender estas absurdas consultas, provocadas por un diseño informático del sistema normalizado de solicitud insuficientemente cuidado).

4.5. Impedir dar por terminada la solicitud y presentarla si no se cumplimentan los campos marcados como obligatorios en el formulario o no se hace convenientemente

Considero que es un factor de incremento de carga administrativa el que un sistema normalizado de solicitud pueda hacer depender la finalización o presentación de la solicitud, de consideraciones estrictamente formales aplicadas a la información proporcionada por el usuario. Por eso en el epígrafe me refiero deliberadamente a cumplimentar convenientemente los campos (conveniencia vs corrección). Si el sistema normalizado de solicitud criba los datos aportados por el interesado con parámetros estrictamente formales, puede terminar rechazando la información aunque sea verdadera (ejemplo del campo «cuerpo», que inadmitía la respuesta «catedráticos de universidad», o el campo «Facultad», que rehusaba «Facultad de Derecho» o «Derecho»). Hay que subrayar que estos filtros de datos están configurados en atención a criterios formales de pura normalización, preocupados solo por la carga de trabajo de la Administración, y ello sólo es jurídicamente aceptable, considero, en la medida en que no restrinja las libertades, derechos y garantías del solicitante.

Para abundar en esta línea es necesario discernir entre los datos que obligatoria o imprescindiblemente hay que proporcionar a la Administración para que ésta de curso a la solicitud y los que son imprescindibles para acceder al registro, pues no tienen por qué coincidir, y por consiguiente, no merece igual trato la omisión de uno y la de otro. Por eso en el art. 71 de la Ley 30/1992 se prevé la subsanación de solicitudes, mediante un plazo de diez días hábiles que debe otorgarse al interesado para la aportación de los datos relativos a «los requisitos que señala el artículo [70] y los exigidos, en su caso, por la legislación específica aplicable» que no se hayan acompañado a la solicitud, so pena de aplicar el desistimiento. En consecuencia, puede entenderse que los datos imprescindibles para la admisión en registro son los indispensables para poder cursar un requerimiento de subsanación (sería abusivo calificar un campo como obligatorio con otro criterio), y que, de faltar cualquier otro, lo que procede es recepcionar por registro y solicitar subsanación.

Sin embargo, en muchas ocasiones se obvia esta diferenciación cuando se aplican las nuevas tecnologías al trámite de solicitud con el resultado de ningunear el derecho a subsanarlas previsto en la Ley 30/1992, que también rige en las relaciones jurídicas de carácter electrónico[25] y que proyecta una intensa duda de ilegalidad sobre los reglamen-

25 El art. 4.d de la Ley 11/2007 exige que la utilización de las tecnologías de la información por la Administración se ajuste, entre otros, al "Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común". En la conclusión de que el derecho de subsanar escritos y

tos que permiten que los registros electrónicos rechacen solicitudes con campos incompletos[26]. En efecto, si el hecho de no completar un dato relativo a un requisito exigido por la norma reguladora de lo solicitado supone no poder guardar los datos de la solicitud, no poder avanzar en su cumplimentación, ni tampoco poder confirmar o generar la solicitud para luego presentarla en registro, a la Administración se le estará asegurando la perfección formal en todas las solicitudes que reciba, y se les estará ahorrando costes de trabajo al no tener que cursar requerimientos de subsanación ni de comunicaciones de eventuales desistimientos por no atender el requerimiento en plazo, pero todo ello será a costa del derecho del ciudadano, a quien un sistema normalizado le arrebatará la libertad de ejercer cuando estime oportuno su derecho, presentando su solicitud y en su caso, subsanando la solicitud de acuerdo con el art. 71.1 de la Ley 30/1992.

Si esto es así en términos generales, cuando la presentación del escrito o solicitud está condicionada jurídicamente a ser realizada dentro de un plazo dado y la utilización de medios electrónicos es preceptiva, entonces, además de estar vulnerándose derechos legales del ciudadano frente a la Administración, se le está incrementando la presión burocrática (generando «miedo al papeleo») y se perjudica el ahorro de carga administrativa potencialmente ofrecido por las nuevas tecnologías, y si el administrado no consigue superar *su* problema respecto a los campos obligatorios puede llegar a la situación límite de no poder presentar su escrito, ya que el sistema no le permite confirmar su solicitud con campos obligatorios sin rellenar o con datos declarados formalmente erróneos de forma automática.

4.6. La verificación automatizada de datos por relación a otros campos que implique nuevas exigencias no previstas por la norma reguladora

Si un sistema normalizado de solicitud incorpora la verificación automatizada de los datos incorporados por el usuario con el efecto de negar el acceso a la generación y presentación de la solicitud, esa verificación debe estar configurada con el exquisito cuidado de ajustarse estrictísimamente a las previsiones de la norma reguladora del procedimiento en cuestión. Otra cosa equivaldría a que la Administración responsable del sistema normalizado de solicitud se estuviera arrogando la potestad de modificar, a través de la aprobación del sistema, la norma aplicable que diseña la extensión del derecho del solicitante sin observar el procedimiento legalmente exigible para el cambio normativo.

En estos casos, se conculcan derechos subjetivos del solicitante, evidentemente, pero también se añade carga administrativa, puesto que hay que aplicar tiempo hasta

solicitudes también rige en las solicitudes cursadas electrónicamente por formularios coincido con VALERO TORRIJOS (2007), p. 96 y 97; PALOMAR OLMEDA (2010), p.620.

26 Vgr. art. 29.1.c Real Decreto 1671/2009, de 6 noviembre, de desarrollo parcial de la Ley 11/2007.

lograr descubrir el motivo del rechazo, ya que, generalmente, el sistema no indica expresamente la limitación introducida, sino que simple y comodonamente se niega a guardar datos so pretexto de haber identificado errores.

Sirva de ejemplo el que me comentaba este año el solicitante de una Beca del Programa de Formación del Profesorado Universitario que había intentado pedir su beca con co-directores de Tesis, profesores de la misma Universidad. Me decía que la norma reguladora no lo impedía, pero el sistema, empleando una de estas verificaciones automáticas, sólo se admitía la co-dirección si los profesores pertenecían a Universidades diferentes. El resultado: aparte de perder un tiempo considerable intentando deducir cuál era el problema, tuvo que renunciar a la co-dirección porque de otra manera no se podía generar ni presentar la solicitud.

5. CONCLUSIONES: HACIA LA MATERIALIZACIÓN DE LA REDUCCIÓN CARGAS ADMINISTRATIVAS A TRAVÉS DE SOLICITUDES GENERADAS ELECTRONICAMENTE

A la vista de lo anterior, conviene preguntarse sobre cómo avanzar hacia la efectiva materialización de la simplificación de cargas administrativas en la generación electrónica de solicitudes dirigidas a las Administraciones Públicas. El diseño e integración de modelos o formularios normalizados en sistemas normalizados de solicitud antes de que se pongan a disposición de los ciudadanos en la correspondiente sede electrónica (art. 35 Ley 11/2007) está sometido a requisitos jurídicos (formales y sustantivos)[27] que

27 Al menos en el ámbito estatal, las exigencias jurídicas fundamentales en este sentido podrían sintetizarse en: i) Las exigencias formales de aprobación previa de qué datos van a requerirse y cuáles de ellos serán obligatorios (según se infiere, siguiendo a VALERO TORRIJOS (2007:p.97), de los artículos 25 y 35.1 de la Ley 11/2007); así como el establecimiento mediante Orden Ministerial, previo informe favorable del Ministerio de la Presidencia del los sistemas normalizados de solicitud (art. 5); ii) La exigencia sustantiva de intangibilidad jurídica de la posición de los interesados en cuanto a sus derechos y garantías si los modelos o formularios se integran en sistemas normalizados de solicitud (art. 5 del Real Decreto 772/1999, de 7 de mayo). No otra cosa quiere asegurar este precepto cuando lo condiciona a «que se garantice el cumplimiento de los requisitos contemplados en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, así como en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y las medidas de seguridad informática contempladas en el Real Decreto 1720/2007, de 21 de diciembre». En este sentido similar, por la doctrina, véanse, por todos, las afirmaciones de VALERO TORRIJOS (2007:98).

permiten (y exigen) en un control preventivo de la neutralización del alivio de cargas administrativas. Pero, evidentemente, la mera previsión normativa de estos requisitos no es suficiente.

Poquísima o nula repercusión en el avance que sugerimos podrá aportar el canalizar la evidencia de aumento de carga administrativa que se ha puesto de manifiesto páginas atrás a través de los mecanismos de recurso administrativo o jurisdiccional por parte de los interesados frente a la aprobación de integración de formularios en sistemas normalizados de solicitud, o a su implantación, o frente a los ya disponibles en la sede electrónica (a veces de uso obligatorio), y no sólo por los nuevos costes económicos que implicarían estos recursos sino también por las dificultades de prueba que habría que superar. Puede adivinarse que el resultado será igualmente insatisfactorio si la reacción se vehicula mediante quejas o sugerencias a la Administración responsable del sistema normalizado de solicitud. A un muy mínimo porcentaje de usuarios le quedará tiempo y ganas, después de haberse enfrentado a una solicitud de generación electrónica deficientemente diseñada, de emplear más tiempo y energías en preparar una queja o una sugerencia. Uno se siente engañado al descubrir en estas aplicaciones un «caramelo envenenado», una oferta de reducción de cargas que se transforma al ir a disfrutarla en un laberinto de trampas informáticas. Y se le genera la duda de si se utiliza la administración electrónica para hacerle claudicar de su derecho a solicitar, y la certeza de que su tiempo y sus necesidades son despreciadas por la Administración.

El camino tiene que ser otro. El compromiso político por la reducción de cargas administrativas requiere un cambio de actitud por parte de la Administración para que asuma realmente su carácter servicial de los intereses generales y de los del ciudadano en particular (art. 103 CE) que le haga rechazar toda neutralización de carga administrativa en la implementación de los procedimientos administrativos. Es necesario que la propia Administración sea consciente del despilfarro de todo orden que implica que la simplificación administrativa alcanzada normativamente pueda arruinarse porque en la fase de implementación la Administración no esté atenta a los factores de perversión del alivio de cargas que se esconden en las nuevas tecnologías. Si se quiere que la minimización de cargas administrativas sea una realidad, la Administración no puede contentarse con obtener ventajas para ella en términos de reducción de costes de trabajo en la gestión y tramitación de los procedimientos a los que aplica medios electrónicos, sino que ha maximizar las ventajas de la tecnología para que alcancen también al usuario, cuyos impuestos nutren los presupuestos generales. La valentía de aceptar que el carácter no indemnizable de las «meras molestias» (que pueden considerarse las cargas administrativas), no es excusa ni habilita a provocarlas caprichosamente, impulsará el avance.

Se necesita, en definitiva, que se incentive en la Administración y en sus empleados la preocupación por atender bien al ciudadano y no sólo aparentarlo. Y en concreto, en relación con la aprobación de formularios normalizados y el establecimiento de sistemas normalizados de solicitud es imprescindible una auténtica verificación de que su dise-

ño no da al traste con el esfuerzo realizado por acomodar el ordenamiento jurídico al principio de simplificación de cargas, de manera que antes de obligar a los usuarios a su empleo se confirme, entre otros, que:

- se puede visualizar el conjunto de campos antes de empezar a volcar datos en la solicitud.
- se distinguen los campos obligatorios (condición para que se tramite) y los campos esenciales para la admisión por registro (que han de ser únicamente no subsanables).
- se seleccionan como campos obligatorios sólo los relativos a requisitos sustantivos.
- se puede generar y presentar la solicitud aunque los campos obligatorios se dejen sin rellenar, garantizando el derecho de subsanación.
- la normalización de contenidos posibles para los distintos campos (sin buscadores poco inteligentes o con desplegable de opciones) resulta inocuo.
- la verificación interna de datos aportados no supone incorporar requisitos no previstos en la regulación.

6. BIBLIOGRAFÍA BÁSICA

Betancor (2009): *Mejorar la regulación. Una guía de razones y medios.* Madrid: Marcial Pons & Fundación Rafael del Pino.

Canals i Ametller, D. (2010) «Mejora Normativa y Reducción de Cargas Administrativas». *Informe Comunidades Autónomas.* Barcelona: Institut de Dret Públic. 43-67.

Mora Ruiz, M (2014): «Metodología y organización administrativa de la simplificación de procedimientos» en Gamero Casado (Ed): *Simplificación del procedimiento administrativo y mejora de la regulación: Una metodología para la eficacia y el derecho a la buena administración.* (77-117) Valencia: Tirant Lo Blanc.

Palomar Olmeda (2010): en Gamero y Valero (Eds): *La Ley de Administración Electrónica: Comentario sistemático de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.* Cizur Menor: Aranzadi-Thomson Reuters. (597-757).

Rego Blanco, M.D (2014):: «Las cargas administrativas: concepto y régimen jurídico para su reducción» en AAVV *Simplificación del procedimiento administrativo y mejora de la regulación: Una metodología para la eficacia y el derecho a la buena administración.* (239-282) Valencia: Tirant Lo Blanc.

Valero Torrijos (2007): *El régimen jurídico de la e-Administración; El uso de medios informáticos y telemáticos en el procedimiento administrativo común.* Granada: Comares. (2ª ed).

AMMINISTRAZIONE DIGITALE E TRASPARENZA NELL'ORDINAMENTO ITALIANO

Enrico Carloni
Professore associato di diritto amministrativo nell'Università degli studi di Perugia

ABSTRACT: Il decennio che ci lasciamo alle spalle costituisce, per l'amministrazione italiana, un decennio fondamentale per la definizione di un diverso modello di relazione con i cittadini, reso possibile dal web. Dal punto di vista del diritto, in questo decennio vengono approvate leggi molto importanti, che definiscono il nuovo «statuto» dell'amministrazione elettronica: dal Codice dell'amministrazione digitale, 2005, fino al Decreto «Trasparenza», 2013, assistiamo in primo luogo dal punto di vista normativo ad un formidabile impulso all'evoluzione del modello italiano di amministrazione.

Dal punto di vista dell'eGovernment, la legge italiana in materia (del 2005) è stata più volte corretta ed integrata, da ultimo nel quadro di riforme volte ad accelerare la piena digitalizzazione del sistema pubblico e a rafforzare alcune linee di sviluppo prioritarie inquadrate nella «Agenda digitale italiana». Questa accelerazione produce, al momento, risultati ancora incompleti, ma presenta problemi rilevanti, legati all'idea di una possibile erogazione di servizi pubblici esclusivamente on line (principio di esclusività, con connesse problematiche di digital divide).

Dal punto di vista della trasparenza, questa diviene sempre più una trasparenza «on line», attraverso attività di pubblicità attiva, nei siti istituzionali. Questo nuovo modello di trasparenza, che vede in numerosi obblighi di pubblicazione il principale strumento di conoscibilità, è stato sviluppato compiutamente nel 2013 nel quadro della nuova disciplina anti-corruzione. Questo modello, del quale vengono illustrati i caratteri, collega eGovernment e trasparenza nella prospettiva di un'amministrazione aperta, al servizio del cittadino, ed inquadra dunque il modello italiano (quanto ad aspirazioni) nel contesto dell'open government e dell'open data government.

PAROLE CHIAVE: Italia; eGovernment; Amministrazione digitale; Trasparenza; Open government; Open data; Anti-Corruzione; Servizi in rete; Digital divides.

1. INTRODUZIONE

Il decennio che ci lasciamo alle spalle costituisce, per l'amministrazione italiana, un decennio fondamentale per la definizione di un diverso modo di rapportarsi con i cittadini, e la «amministrazione digitale» diventa, in questo periodo, la prospettiva di sviluppo e modernizzazione del sistema pubblico. Dal punto di vista del diritto, in questo decennio vengono approvate e trovano attuazione leggi molto importanti, che definiscono il nuovo «statuto» dell'amministrazione elettronica. Dal Codice dell'am-

ministrazione digitale, del 2005, fino al Decreto «Trasparenza», del 2013, assistiamo in primo luogo dal punto di vista normativo ad un formidabile impulso all'evoluzione del modello italiano di amministrazione pubblica.

Amministrazione elettronica e trasparenza sono due angolazioni dalle quali è possibile esaminare questo sviluppo, e queste diverse prospettive convergono nell'idea di *open government*, che le raccoglie ma non le esaurisce. La trasformazione del rapporto tra amministrazioni e cittadini risiede, come visto, in modo rilevante, nell'applicazione delle tecnologie dell'informazione e della comunicazione all'azione ed all'organizzazione delle amministrazioni pubbliche: lo sviluppo dell'open government si intreccia, dunque, inevitabilmente, a quello dell'*eGovernment* (per «*electronic*» *government*), che rimanda appunto a questi processi di trasformazione del sistema pubblico, nei quali l'utilizzo delle Ict è diffuso e generalizzato nella prospettiva di un miglioramento dell'efficienza e della trasparenza dell'azione pubblica.

L'idea, che ricollega strettamente i concetti di *eGovernment* ed *open government*, è che il ricorso a queste dinamiche possa rendere il sistema amministrativo non solo più produttivo, ma anche più aperto e partecipativo (Comunicazione della Commissione UE, *Il ruolo dell'eGovernment per il futuro dell'Europa*, COM (2003) 567). Un approccio, questo, che a livello legislativo è chiaramente esplicitato nel disegno della «Agenda digitale»: tra i compiti affidati dal d.l. 5 del 2012 alla «Cabina di regia» per l'Italia digitale troviamo, infatti l'art. 47 del decreto individua tra gli obiettivi dell'Agenda digitale non solo, in modo marcato, l'open data (il decreto parla di «*promozione del paradigma dei dati aperti (open data) quale modello di valorizzazione del patrimonio informativo pubblico, al fine di creare strumenti e servizi innovativi*»), ma soprattutto prevede (coma 2 bis, lett. c) del decreto), il «*potenziamento delle applicazioni di amministrazione digitale (e-government) per il miglioramento dei servizi ai cittadini e alle imprese, per favorire la partecipazione attiva degli stessi alla vita pubblica e per realizzare un'amministrazione aperta e trasparente*». L'eGovernment è individuato dunque, in modo esplicito, come fondamentale leva di sviluppo del paradigma dell'open government.

L'evoluzione di questo processo passa, nell'esperienza (non solo) italiana, per fasi diverse: una prima, caratterizzata da sperimentazioni locali (le c.d. «reti civiche»); una seconda, nella quale a guidare le trasformazioni sono politiche *top down* che coinvolgono le diverse amministrazioni anche grazie ad importanti finanziamenti pubblici (attraverso i c.d. Piani di *eGovernment*, che si inscrivono appunto nel quadro delle politiche europee); una terza, nella quale diventa rilevante se non prevalente la regolazione legislativa del fenomeno. E' quest'ultima la fase che caratterizza il decennio appena trascorso ed ha il suo passaggio fondamentale nel d.lgs. n. 82 del 2005, codice dell'amministrazione digitale, del 2005; nella «stagione della crisi» degli ultimissimi anni, sta emergendo una quarta fase, quella attuale, nella quale prevalgono le esigenze di assicurare una guida alle politiche di innovazione nel loro complesso e si susseguono interventi legislativi di

completamente e correzione, che ruotano intorno ad una pluralità di poli tenuti insieme dal disegno (tuttora abbastanza confuso) della c.d. Agenda digitale.

A valle di un processo di regolazione che ha assunto, nel corso dell'ultimo triennio, un ritmo incalzante, il disegno riformatore ha acquisito una sua fisionomia, ma il disegno rischia di perdersi nella complessità e stratificazione delle normative, mentre attende peraltro di essere messo a regime da una serie di provvedimenti attuativi e di politiche di implementazione.

Lo scenario della digitalizzazione pubblica risulta, in ogni caso, un tema che richiede di essere approfondito, per cogliere le implicazioni, e i collegamenti reciproci, tra la dimensione normativo-tecnologica, contenuta nel Codice dell'amministrazione digitale, e quella più propriamente «politica» che si traduce a livello legislativo anzitutto nell'apertura alle sfide ed alle prospettive dell'open government, inteso in particolare come trasparenza totale ed open data government.

La combinazione della disciplina in materia di digitalizzazione (il Codice dell'amministrazione digitale, ed i successivi provvedimenti tra i quali in particolare il decreto «Crescita 2.0») e di trasparenza (con il d.lgs. n. 33 del 2003), va a costruire la struttura fondamentale di regolazione del «data government» nell'amministrazione italiana, cui si aggiungono almeno altre due regolazioni importanti, quella in materia di Privacy (d.lgs. n. 196/2003, Codice della privacy) e di riutilizzo dei documenti (PS, d.lgs. n. 36/2006). Il governo dei dati è rilevante sia in una prospettiva «interna» (al sistema pubblico, e alle singole amministrazioni) ed in questo senso trova la sua disciplina anzitutto nel codice dell'amministrazione digitale, ed in una prospettiva «esterna», che attualmente richiama anzitutto il fenomeno dell'open data government, regolato ora soprattutto dal decreto «trasparenza» (d.lgs. n. 33/2013), ma con importanti previsioni nel Cad.

2. L'AMMINISTRAZIONE DIGITALE A (QUASI) DIECI ANNI DAL SUO CODICE

Una delle regolazioni centrali per l'affermazione di un nuovo modello di relazione tra amministrazioni e cittadini e, per quello che qui più direttamente interessa, di trasparenza e partecipazione, è il Codice dell'amministrazione digitale: approvato nel 2005 (d.lgs. n. 82) e modificato nel 2006 e quindi riformato nel 2010 (d.lgs. n. 235/2010) e nel 2012 (d.l. 179/2012, convertito in l. 221/2012), il codice prevede standard e regole che mirano a rendere effettiva la «proiezione» digitale delle pubbliche amministrazioni e, progressivamente, a rendere ordinaria ed esclusiva l'azione mediante Ict.

L'attività amministrativa mediante Ict trova, dunque, nel Cad la sua affermazione, ma il principio, che a questo si collega, di «normalità», se non preferenza, per il ricorso alle tecnologie informatiche nelle relazioni tra amministrazioni e cittadini, è stato negli stessi tempi (con la l. 15 del 2005) inserito nel cuore della disciplina dell'attività am-

ministrativa, la legge 241 del 1990, con l'art. 3 *bis* («Uso della telematica»), in base al quale «*per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*».

In questo contesto, il Cad, in sintesi, «*promuove e regola la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione e nei rapporti tra amministrazione e privati*» (si v. le *Linee guida per i siti web delle p.a.*, 2011).

Si tratta di un testo normativo molto ampio (92 articoli), oggetto di successivi ritocchi e di una significativa «messa a punto» (nel 2010) che contiene, oltre alle parti di cui si è detto relative alla documentazione amministrativa, una serie di affermazioni di principio, relative in particolare ai diritti all'uso delle Ict ed all'organizzazione della funzione (Capo I, artt. 1-19) ed una parte relativa ai dati, ai siti delle pubbliche amministrazioni ed ai servizi on line (art. 50 - 66). Oltre a queste parti, sulle quali ritorneremo, troviamo articoli dedicati allo sviluppo dei sistemi informatici delle p.a. (artt. 67 – 70), alle modalità di formazione delle «regole tecniche» che sono fondamentali nell'impianto della legge (art. 71), ed infine alla disciplina della «rete» tra le amministrazioni, il «sistema pubblico di connettività – Spc» (artt. 72-87).

Nel complesso, la digitalizzazione pubblica è vista come un fattore di modernizzazione, e di trasformazione del rapporto tra amministrazioni e cittadini.

2.1. I diritti all'uso delle Ict e i divides digitali

Una sezione importante del Codice, innovativa e rilevante per fare del Cad uno «statuto» del cittadino digitale (enfaticamente il governo, nell'adottare il provvedimento, parlava di *Magna Charta* dell'amministrazione digitale: Belisario, 2009, 9), è quella relativa ai diritti all'uso delle Ict, cui è utile dedicare una (pur breve) attenzione.

Il primo diritto previsto dal Codice, all'art. 3, è quello di portata più generale, all'uso delle tecnologie (del quale, in sostanza, gli altri «diritti» costituiscono una specificazione»). In base a quanto previsto dall'art. 3, «*i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni», anche se questo pur sempre «ai sensi» (e quindi nei limiti) «di quanto previsto dal presente codice*».

Tramite queste previsioni, si va dunque affermando una nuova concezione dell'uso delle Ict da parte delle amministrazioni: l'*eGovernment*, da «semplice» questione organizzativa interna arriva a qualificarsi come «diritto degli utenti» (Bonomo, 2012). Si tratta, quale che sia la qualificazione di queste situazioni soggettive, di questioni rispetto alle quali la competenza spetta al giudice amministrativo (art. 3, comma 1 ter del Cad).

Sono, queste, a ben vedere, situazioni giuridiche «condizionate» (non solo ai sensi del codice, ma anche dal potere organizzatorio delle pubbliche amministrazioni), che però si sostanziano in alcuni casi in legittime pretese che il cittadino può far valere nei confronti delle pubbliche amministrazioni: così, è facoltà del cittadino individuare un proprio «domicilio digitale» (art. 3 bis) e «*le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato [ ]. Ogni altra forma di comunicazione non può produrre effetti pregiudizievoli per il destinatario*». E', questa, una facoltà che, se utilizzata, può consentire una forte semplificazione nei rapporti tra amministrazioni e cittadini (specie, in effetti, laddove si tratti di soggetti organizzati ed in relazione assidua con l'amministrazione).

Così il codice prevede il diritto alla partecipazione al procedimento ed ad effettuare pagamenti mediante Ict, a comunicare con la p.a. mediante posta elettronica certificata.

In sostanza, attraverso queste previsioni si pongono le premesse per una relazione mediante Ict valida a tutti gli effetti, e se ne promuove la diffusione.

Più problematiche quelle previsioni (introdotte di recente) con le quali l'uso delle Ict diventa, per i privati, non una facoltà ma un obbligo (e dove, quindi, il Cad sposa la linea della «esclusività» digitale, in base alla quale taluni rapporti con la p.a. possono realizzarsi solo mediante Ict). E' il caso dell'art. 5 *bis* del codice, in base al quale «*la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene* esclusivamente *utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.*»

Se teniamo conto del fatto che «imprese» sono anche quelle individuali, agricole, sociali, ne ricaviamo l'impressione di una pericolosa (e poco semplificante) accelerazione, specie se consideriamo un problema spesso trascurato quale quello dei (tuttora persistenti) *divides* digitali.

Rispetto ai problemi che impediscono la piena eguaglianza digitale tra i cittadini, che sono di tipo sociale (pensiamo all'età), culturale (il livello di istruzione), economico (il costo di attrezzature e connessione), tecnologico (l'assenza di una completa copertura del paese con reti a banda larga), il codice non contiene in effetti che una scarna previsione, contenuta nell'art. 8, relativa alla alfabetizzazione dei cittadini, in base alla quale «*lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni*».

Una previsione, questa, recentemente ribadita dal decreto Crescita 2.0 (d.l. 179 del 2012, convertito in l. 221 del 2012), in base al quale lo Stato, nel rispetto del principio di leale collaborazione, «*favorisce, tramite azioni concrete, l'alfabetizzazione e lo sviluppo delle competenze digitali con particolare riguardo alle categorie a rischio di esclusione*» (art. 1). Una previsione, quest'ultima, che più che innovare il quadro normativo dei principi

in materia di riduzione del *digital divide* svolge il ruolo di collegare questa problematica, dell'inclusione digitale, all'interno delle politiche (ed alle risorse) dell'Agenda digitale italiana.

2.2. I servizi in rete e il principio di «esclusività»

Il «modello» da cui prendere le mosse è quello, definito attraverso l'attuazione dei piani di eGovernment dei primi anni del secolo (l'Action Plan italiano è del 2000), su cui si basa questo approccio è quello di un sistema pubblico nel suo complesso integrato, nel quale la dimensione digitale è strumento di efficienza e semplificazione nelle relazioni con i cittadini. Esemplare, in questo senso, l'approccio per il quale i servizi sono riferiti ad «eventi della vita» del cittadino e dell'impresa, e per la loro erogazione il cittadino accede ad un'amministrazione di *front office* che è però potenzialmente diversa da quella che materialmente è responsabile della fornitura del servizio (come *back office*): pensiamo ad esempio al fatto di accedere, tramite il proprio comune, a servizi relativi al rilascio della patente di guida che dipendono dagli uffici della motorizzazione civile. Questo disegno, definito nei documenti del periodo come «federalismo informatico», si scontra con vari problemi, tra i quali in particolare la difficoltà di integrazione tra amministrazioni e livelli di governo diversi, tanto più alla luce della riforma del Titolo V della Costituzione che rafforza l'idea di approcci autonomi e differenziati a livello locale (per quanto, nel Titolo V, si riservi pur sempre allo Stato la competenza in materia di «*coordinamento informativo statistico ed informatico dei dati*» con l'art. 117, comma 2, lett. r), della Costituzione).

Nel Codice dell'amministrazione digitale, la disciplina dei servizi in rete è contenuta anzitutto nell'art. 63, che regola la «organizzazione e finalità dei servizi in rete», prevedendo, per le pubbliche amministrazioni centrali, il dovere di individuare modalità di erogazione dei servizi mediante Ict «*in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di uguaglianza e non discriminazione*» (comma 1).

La piena «transizione al digitale» è disciplinata anche dal comma 3 *bis* del Cad, introdotto dal d.l. 5/2012, ai sensi del quale «*a partire dal 1 gennaio 2014*» le amministrazioni pubbliche ed i gestori di servizi pubblici (centrali, ma anche regionali e locali) «*utilizzano esclusivamente i canali e i servizi telematici*» per l'utilizzo dei propri servizi «*anche a mezzo di intermediari abilitati, per la presentazione da parte degli interessati di denunce, istanze e atti e garanzie fidejussorie, per l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi, nonché per la richiesta di attestazioni e certificazioni*» (art. 63, comma 3-*bis*). Inoltre, a partire dalla stessa scadenza, le amministrazioni utilizzano «*esclusivamente i servizi telematici […] anche per gli atti, le comunicazioni o i servizi dagli stessi resi*» (art. 63, comma 3-*ter*).

Questo «principio di esclusività» è dunque assunto come criterio generale, suscettibile di eccezioni e limitazioni (da definire con decreto del Presidente del consiglio dei Ministri, così come previsto dallo Cad).

3. IL NUOVO MODELLO DI TRASPARENZA

La frontiera su cui si concentra in modo particolare l'attenzione del legislatore diventa però, nel corso dell'ultimo quinquennio (dalle riforme «Brunetta» del 2009 a quelle del governo Monti e in parte Letta), ancor più che quella dei servizi, quella della trasparenza, resa possibile attraverso l'utilizzo delle Ict ed in particolare della rete Internet.

La trasparenza, come condizione frutto di una serie di istituti e meccanismi, ha tradizionalmente trovato forza in primo luogo attraverso il riconoscimento in capo al cittadino (sia che si pensi ad un generico individuo, a «chiunque», sia che si pensi a soggetti qualificati, quali ad esempio i giornalisti) del diritto di «andare a vedere», vale a dire di un diritto a conoscere, ad accedere alle informazioni od ai documenti in mano pubblica, questo, in Italia, a partire dalla legge sul procedimento amministrativo, n. 142 del 1990.

Ci muoviamo, in questi casi, in una dimensione di trasparenza «passiva», vale a dire entro modelli nei quali è il cittadino a rivolgersi all'amministrazione, per conoscere, mentre un discorso diverso si pone, tradizionalmente, con riferimento ai doveri di divulgazione, diffusione (la c.d. *dissemination*) di informazioni da parte dei soggetti pubblici: Internet muta in parte questo paradigma concettuale, avvicinando le due dimensioni della trasparenza «attiva» e «passiva», ma la distinzione resta tuttora utile, anche se il confine diviene via via più sfumato (basti pensare alle informazioni accessibili tramite la rete Internet in apposite sezioni dei siti, secondo un modello non distante da quello delle *reading room* americane previste dall'eFoia, *Electronic Freedom of Information Act*: aree dei siti istituzionali dove sono posti gli atti di maggiore interesse o quelli più frequentemente oggetto di istanze di accesso).

Questa «continuità» tra l'area dell'accesso (trasparenza «passiva») e quella della pubblicità (trasparenza «attiva») è possibile, evidentemente, nella misura in cui il diritto a conoscere sia riconosciuto a tutti i cittadini, cosicché ciò che cambia è soltanto la modalità (più idonea) di messa a disposizione delle informazioni. Quanto più, invece, il novero dei legittimati a conoscere (attraverso l'esercizio del diritto di accesso) è circoscritto, e quanto più l'amministrazione valuta il *need to know* sulla base delle motivazioni che lo reggono, tanto più questa continuità si perde, e diritto di accesso e pubblicità divengono due strumenti distanti, non comunicanti. Nell'esperienza italiana, come vedremo, questa distanza è particolarmente marcata, per quanto in alcuni ambiti circoscritti i due meccanismi tornino a raccordarsi (come avviene nel campo dell'informazione ambientale, o grazie all'istituto dell'acceso civico). L'analisi dell'esperienza italiana è interessante, e costituisce un riferimento anche per riflettere sulla più recente normativa spagnola, dove diritto di accesso e «pubblicità attiva» costituiscono gli strumenti volti ad assicurare una più ampia trasparenza delle istituzioni pubbliche.

La chiusura, in funzione di tutela «pre (o para) processuale» del singolo, del diritto di accesso, operata dalla legge n. 15 del 2005 a completamento di un percorso di «distanziamento» dal modello Foia, ha segnato lo sganciamento della trasparenza amministrativa dal diritto di accesso, sino ad allora inteso quale principale meccanismo

chiamato ad assicurare la conoscibilità dell'azione dei pubblici poteri. Questa esigenza, non trova sviluppo in una legislazione coerente con il modello del *freedom of information* (e quindi con forme di trasparenza «passiva»), ma nel progressivo affermarsi di forme di pubblicità, attraverso la diffusione di informazioni (individuate dal legislatore) attraverso i siti istituzionali delle amministrazioni.

Dal 2005 in poi, in un crescendo, in ogni legge o manovra finanziaria possiamo riscontrare nuove previsioni di «elementi conoscitivi» dei quali il legislatore richiede la disseminazione attraverso la rete: una stratificazione della quale il governo, con il ministro Brunetta, in prima battuta terrà conto, attraverso la c.d. «Operazione trasparenza», e che lo porterà poi, in un secondo tempo, ad «istituzionalizzare» questo nuovo modello di relazione tra amministrazioni e cittadini, attraverso le riforme legislative del 2009. Centrale risulta, nell'affermazione ed emersione del nuovo modello, il combinato delle previsioni contenute già nel Cad («contenuti obbligatori dei siti») e quindi nella legge n. 15 e nel d.lgs. n. 150 dello 2009 (c.d. «Riforma Brunetta»).

Questo nuovo modello viene compiutamente esplicitato dall'art. 11 del decreto legislativo 27 ottobre 2009, n. 150, che definisce la trasparenza come «*accessibilità totale, anche attraverso lo strumento della pubblicazione sui siti istituzionali delle amministrazioni pubbliche, delle informazioni [ ] allo scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità*».

Come ha evidenziato la Commissione per la valutazione, l'integrità e la trasparenza delle p.a. (Civit, ora Apac), attraverso una serie di leggi che individuano doveri di pubblicare numerose informazioni *on line*, si viene così definendo un'idea di trasparenza che riflette «*una nozione diversa da quella contenuta negli articoli 22 e seguenti della legge 7 agosto 1990, n. 241*»: un'idea di trasparenza come «accessibilità totale» che presuppone, come già evidenziato, l'accesso da parte dell'intera collettività «*a tutte le informazioni pubbliche, secondo il paradigma della libertà di informazione dell'open government*» (delibera Civit n. 105 del 2010, *Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità* (previste dall'articolo 13, comma 6, lettera e), del decreto legislativo 27 ottobre 2009, n. 150).

Questo modello, di trasparenza come accessibilità totale, ha trovato pochi anni dopo un ulteriore sviluppo, in un disegno maggiormente organico, con la legge anticorruzione, n. 190 del 2012, e soprattutto con il successivo d.lgs. n. 33 del 2013 (cd. codice della trasparenza). Una disciplina, questa, con la quale «*la trasparenza diventa la condizione normale di esistenza e di azione delle pubbliche amministrazioni e non è più perseguita da norme singole, ma è l'oggetto di una disciplina di sistema*» (Casetta-Fracchia, 2013, 67).

3.1. Trasparenza e integrità nella legge «anticorruzione»

Sin dalla metafora della luce del sole come «migliore disinfettante», la trasparenza è vista come funzionale al contenimento dei fenomeni di malcostume e di corruzione: intesa, questa, sia in senso «tecnico», come specifico reato previsto dal codice penale,

che in senso più lato, nella sua accezione amministrativistica (Mattarella, 2013), come «*maladministration*». In quest'ultima accezione, la corruzione si lega alle condotte che minano l'integrità del dipendente e, quindi, inficiano le sue condotte slegandole dalla cura dell'interesse pubblico.

Si tratta di una relazione, quella tra trasparenza ed integrità (o, volendo, trasparenza vs corruzione), che assume nel corso dell'ultimo quinquennio una valenza, prima in termini di affermazione di principio, poi con l'adozione di atti normativi e presidi organizzativi più stringenti, crescente, per coronare nella legge anticorruzione (l. 190 del 2012) e nei provvedimenti attuativi.

Queste innovazioni, recenti, rafforzano il legame, stringente, tra trasparenza ed integrità che era stato ben evidenziato, dalla Civit (ora Anac, Autorità nazionale anti corruzione), già in occasione della delibera n. 105 del 2010: «*con riferimento alla legalità e alla cultura dell'integrità, la pubblicazione di determinate informazioni pubbliche risulta strumentale alla prevenzione della corruzione nelle pubbliche amministrazioni*».

In ogni caso, la «via della trasparenza» al contrasto della corruzione è ben presente al legislatore, se è vero che nella legge in materia (l. 190 del 2012) è prestata grande attenzione alla trasparenza dell'attività amministrativa, attraverso un articolo che prevede che «*la pubblicazione, sui siti istituzionali delle pubbliche amministrazioni, delle informazioni relative ai procedimenti amministrativi, secondo criteri di facile accessibilità, completezza e semplicità di consultazione*», con particolare riferimento ai procedimenti concorsuali, di scelta dei contraenti, di autorizzazione e concessione, di sovvenzione. La trasparenza si lega, dunque, in modo significativo alla prospettiva del rafforzamento all'integrità ed alla legalità, come rimarcato, peraltro, già nella Convenzione Onu contro la corruzione, del 31 ottobre 2003, ratificata in Italia con la l. n. 116 del 2009.

La legge n. 190 si occupa di «trasparenza» in vari commi dell'art. 1 (che costituisce sostanzialmente l'intera legge, di 83 commi): i commi 15 e 16, che individuano la trasparenza *on line* come «livello essenziale delle prestazioni» e ne fissano alcuni caratteri e contenuti; i commi 35 e 36 che prevedono una delega per l'adozione di un testo unico in materia di trasparenza (in ossequio alla quale è stato adottato il c.d. «codice della trasparenza», d.lgs. n. 33 del 2013) e quindi i principi e criteri da seguire nella sua approvazione.

Quanto ai caratteri della «nuova» trasparenza, il comma 15 chiarisce che questa è assicurata «*mediante la pubblicazione, nei siti web istituzionali delle pubbliche amministrazioni, delle informazioni relative ai procedimenti amministrativi, secondo criteri di facile accessibilità, completezza e semplicità di consultazione, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio e di protezione dei dati personali*».

3.2. Il «codice della trasparenza»

L'approvazione, recente, del decreto delegato, n. 33 del 2013, costituisce un punto di arrivo e, al contempo, di partenza. Un punto di arrivo rispetto a questo processo di

costruzione di un nuovo modello di trasparenza come «accessibilità totale»; un punto di partenza verso l'affermazione di un'amministrazione effettivamente aperta (nei limiti e nel quadro delle potenzialità del decreto). Ai sensi del codice della trasparenza, questa (che riformula la definizione già contenuta nel d.lgs. 150/2009) è «*intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*».

L'ampiezza del novero delle informazioni (riferite all'organizzazione ed all'attività), la finalità di «controllo diffuso» (sul perseguimento delle funzioni e l'uso delle risorse), segna un'evoluzione del concetto, già ricco, di «accessibilità totale» previsto dalla riforma del Ministro Brunetta. Si tratta di un principio (di trasparenza «totale»), che si sviluppa pur sempre nel rispetto dei tradizionali limiti alla conoscibilità (segreti e riservatezza), ma che vuole dare attuazione ad una serie di principi costituzionali che costituiscono l'architrave dell'ordinamento democratico. Così, ai sensi dell'art. 1, comma 2 (*Principio generale di trasparenza*»), la trasparenza «*concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino*».

In questo contesto, di sviluppo di fondamentali principi costituzionali, le disposizioni del decreto individuano un'ampia serie di obblighi di trasparenza e le modalità per la loro realizzazione. La trasparenza coincide, in questa prospettiva, con il meccanismo della «pubblicazione» (*on line*), da intendere come «*pubblicazione, in conformità alle specifiche e alle regole tecniche*» (in allegato al decreto) «*nei siti istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione*» (art. 2, comma 2).

Il decreto elenca quindi, riprendendo e dando coerenza e compattezza ad un gran numero di previsioni precedenti, oltre che individuandone di nuovi, i dati doverosamente «pubblici» (e da pubblicare nei siti): atti normativi e generali (art. 12), informazioni relative all'organizzazione ed all'attività (Capo II, artt. 13-28), dati sull'utilizzo di risorse pubbliche (Capo III, artt. 29-31) e sui servizi e le prestazioni forniti (artt. 32-36), oltre che informazioni relative a specifici settori. Tra le regole settoriali, cui è qui impossibile dedicare puntuale attenzione, troviamo previsioni di indubbio rilievo: quelle relative ai contratti ed alle opere pubbliche (art. 37), agli atti di governo del territorio ed in materia ambientale (art. 39 e 40), al servizio sanitario nazionale (art. 41), agli interventi straordinari e d'emergenza (42).

Tutti questi dati, in quanto dichiaratamente pubblici, ricadono in un regime di conoscibilità che, in base all'art. 3 («*Pubblicità e diritto alla conoscibilità*»), consiste nel fatto che «*chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riuti-*

lizzarli»: la trasparenza si configura, dunque, come obbligo dell'amministrazione e come diritto del cittadino, che può far valere le sue pretese conoscitive, se non soddisfatte a causa dell'omessa pubblicazione, anche attraverso il ricorso all'accesso civico.

Se scorriamo l'elenco delle informazioni «pubbliche» (e in questo senso, può essere utile prendere visione della tabella dei dati di cui si prevede la necessaria pubblicazione, in allegato al decreto), ne ricaviamo l'idea di una trasparenza ricca di effettive potenzialità conoscitive: le amministrazioni, tanto per esemplificare, sono tenute a pubblicare tutte le informazioni relative a sovvenzioni e prestazioni economiche, contratti e consulenze, affitti attivi e passivi, le schede sintetiche di tutti i provvedimenti, i concorsi, le attività di controllo, bilanci ed atti collegati, i costi di produzione dei servizi, le spese per il personale, le relative valutazioni, gli atti di pianificazione e governo del territorio, ecc.

Il recente codice della trasparenza (d.lgs. 33 del 2013) contiene ora una nuova ipotesi di accesso con finalità conoscitive, denominato «accesso civico» (art. 5). E' una previsione suggestiva, specie se letta unitamente alle diffuse critiche alla disciplina italiana del diritto di accesso e, dunque, alla tensione verso il riconoscimento a «chiunque» di un «diritto civico alla pubblicità» (Marzuoli, 2008; Merloni, 2008; Cudia, 2009). Si tratta di un'ipotesi che, per quanto interessante, è volta a rendere effettivo il sistema di trasparenza come pubblicazione *on line* delle informazioni sul quale punta molto il d.lgs. n. 33 del 2013 (e sul quale torneremo), completando e «chiudendo» questo sistema e prevedendo dunque un dovere di far conoscere allorché vi siano state manchevolezze quanto a pubblicazione delle informazioni.

3.3. L'open data government

Con la riforma del Codice dell'amministrazione digitale e più recentemente con il «decreto Crescita 2.0» (d.l. 179 del 2012), il legislatore ha voluto promuovere con forza, a livello normativo, l'*open data*, sollecitando al contempo le amministrazioni ad aprire il proprio patrimonio informativo. Nella sua attuale formulazione, dunque, l'art. 52, comma 1 *bis*, del Cad, prevede espressamente che «*le pubbliche amministrazioni, al fine di valorizzare e rendere fruibili i dati pubblici di cui sono titolari, promuovono progetti di elaborazione e di diffusione degli stessi anche attraverso l'uso di strumenti di finanza di progetto*», utilizzando formati aperti che ne consentano il riutilizzo. Sempre l'art. 52 del Cad, nella prospettiva di favorire l'accesso ai dati ed il loro riutilizzo, dopo la riscrittura operata da d.l. 179, prevede che le pubbliche amministrazioni pubblichino nel loro sito web (nella sezione «Amministrazione trasparente») «*il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso ed i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo*» (comma 1).

In sostanza, attraverso il proprio sito ogni amministrazione dovrebbe rendere conoscibili i *dataset* che detiene, e le condizioni per la loro fruizione. Sempre per favorire al massimo il riutilizzo dei dati, si prevede che, salva diversa espressa indicazione (della necessità di una apposita licenza), «*i dati e i documenti che le amministrazioni titolari*

pubblicano […] si intendono rilasciati come dati di tipo aperto». Il codice dell'amministrazione digitale, infine, all'art. 68 fornisce una serie di definizioni (tra le quali quella di «dato aperto», utili per comprendere la normativa ma anche il fenomeno in sé).

I dati di tipo aperto sono dunque (comma 3, lett. b), i dati che presentano alcune caratteristiche: «1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato»; inoltre «2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati»; ed infine «3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione».

Si tratta di uno sviluppo delle previsioni del decreto n. 36 del 2006, sia perché la disponibilità di *dataset* è orientata non solo alla prospettiva del riutilizzo, ma anche a quella dell'accesso, sia perché si assiste ad una maggiore responsabilizzazione delle amministrazioni rispetto al dovere di rendere disponibili dati, e *dataset*.

Su questa base si innestano iniziative del Ministero per la funzione pubblica (si v. il sito dati.gov.it) che ha promosso la definizione di licenze open data (*Open Data License*) volte alla standardizzazione delle condizioni di disponibilità, oltre che alla «liberazione» e conseguente valorizzazione dei dati pubblici, e che costituisce un punto di riferimento per la conoscenza dei *dataset* resi riutilizzabili ed accessibili da parte delle diverse amministrazioni. Scorrendo l'elenco dei *dataset* disponibili, e delle applicazioni per la loro fruizione (a fini commerciali e non: sempre in dati.gov.it) si può meglio cogliere la portata di queste previsioni, in primo luogo per lo sviluppo di iniziative imprenditoriali ma non meno in un'ottica di trasparenza.

Dei paradigmi dell'open data, il decreto riprende quindi tanto la «partecipazione universale» (chiunque ha diritto di disporre dei dati pubblici), la piena riutilizzabilità («*senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità*»), in formato che ne renda agevole la fruizione (un «formato di tipo aperto»). Mentre l'art. 68 del Cad indica «in positivo» il contenuto della licenza sulla cui base saranno rilasciati e resi riutilizzabili i dati, l'articolo 7 del d.lgs. 33, che richiama integralmente (sia pure con qualche dubbio interpretativo, risolto però dalla dottrina: Ponti, 2013, 118) quanto previsto dall'art. 68, «*compie la medesima operazione in negativo, individuando le uniche clausole restrittive che devono essere rispettate dai riutilizzatori: rispettare l'integrità dei dati e citare la fonte*» (Ponti, 2013, 119).

3.4. I caratteri del nuovo modello di trasparenza

Si definisce, attraverso questo percorso e queste previsioni, un modello di conoscibilità che assume una serie di caratteri che discendono ora dalle caratteristiche proprie

del web (a partire dall'accessibilità generalizzata) ora dal complessivo progetto riformatore che con il codice della trasparenza porta a compimento e definizione spunti già presenti nella legislazione precedente.

Il disegno, in sintesi, è composto da dieci caratteri, che definiscono la nuova tipologia di trasparenza «totale» (Carloni, 2012) e ne segnano la discontinuità rispetto ad altri modelli di trasparenza (ed in particolare, evidentemente, a quello che si realizza con il diritto di accesso ai documenti):

1) Un'accessibilità generalizzata, riconosciuta a chiunque (nella quale è irrilevante la posizione del soggetto che acquisisce l'informazione). Questa generalizzazione del diritto a conoscere è chiara nella legge, ed è confermata, tra l'altro, dalla disciplina dell'accesso civico (art. 5), che riconosce a «chiunque» il diritto di richiedere le informazioni che dovevano essere pubblicate.
2) L'assenza di mediazioni (anche «temporali») e di spazi di discrezionalità dell'amministrazione (nel valutare le ragioni dell'accesso e nel concedere le informazioni): si tratta infatti di una forma di conoscenza fruibile «*direttamente ed immediatamente, senza autenticazione ed identificazione*» (art. 2, comma 2) e quindi senza «mediazione» da parte della p.a. (e così, di nuovo, per l'accesso civico, che non richiede motivazione). Questa «immediatezza» è duplice: da un lato, porta con sé il superamento di quel (tradizionale) *request-and-wait- for-a-response-approach* che è visto come il «tallone d'Achille» delle dinamiche conoscitive (Herz, 2009; Cerrillo, 2011), dall'altro, il venir meno dello stesso ruolo di *gatekeeper*, di vaglio, di filtro, di controllo dell'amministrazione (particolarmente forte nella disciplina italiana dell'accesso: rispetto all'identità del richiedente, rispetto all'interesse, alla motivazione) (Carloni, 2012). La costruzione del rapporto come obbligo dell'amministrazione, consente di configurare in termini di diritto (alla trasparenza) la posizione del cittadino, il che si traduce nell'impianto della legge in particolare nella figura del diritto di accesso civico.
3) Una piena ed agevole fruibilità, anche come «ricercabilità» tramite motori di ricerca e riutilizzabilità e possibilità di rielaborazione, nella prospettiva di un controllo generalizzato sull'azione pubblica: elemento, questo, che è coerente con i paradigmi dell'*open data government*, ma è valutato in termini fortemente critici dal Garante della privacy perché porta con sé, in particolare, il rischio di una «decontestualizzazione» dei dati.
4) La presenza di informazioni quantitativamente rilevanti, secondo un processo di progressivo ampliamento degli obblighi informativi, e quindi idonee a fornire conoscenze ampie anche se comunque individuate dal legislatore e quindi «tipiche». E' il legislatore, senza che siano previsti meccanismi di flessibilità e di sollecitazione da parte dei cittadini, a definire quali dati sottoporre a regime di pubblicazione obbligatoria: ci troviamo dunque, a ben vedere, di fronte ad un elenco molto ampio, ma frutto di scelte via via stratificatesi nel corso del tempo e quindi riprese dal decreto n. 33 del 2013. Manca, però (e questo è un limite) un chiaro criterio

discretivo, quale la distinzione tra informazioni «essenziali» (da pubblicare) e non essenziali, e mancano meccanismi procedurali idonei a consentire verifiche e modifiche nella prospettiva di un progressivo ampliamento ed adeguamento di quest'insieme alle istanze provenienti dalla società.

5) Il fatto che siamo di fronte, almeno dal punto di vista delle amministrazioni, ad elementi conoscitivi «non-*octroyee*» (non «concessi», ma dovuti): la loro scelta è sottratta all'autonomo apprezzamento della amministrazione, essendo operata direttamente dal legislatore. Le pubbliche amministrazioni possono ampliare, ma non restringere, questo «livello essenziale delle prestazioni» informative che si impone a tutti i livelli di governo. L'assenza di discrezionalità, nell'*an*, nel *quando* e nel *quomodo*, configura questa situazione di doverosità come obbligo rispetto al quale l'amministrazione non ha spazi di manovra, se non appunto nel decidere se arricchire questo insieme di informazioni con altre a propria disposizione.

6) Una forte standardizzazione nelle modalità di disseminazione (con predefinizione del «luogo» di pubblicazione e delle modalità anche tecniche di pubblicazione, di una serie di elementi necessari ed in sostanza di una serie di aspetti relativi al «come» e non solo al «cosa» rendere conoscibile): aspetti definiti, in particolare, dall'allegato al decreto che fornisce una «griglia» di organizzazione delle modalità di veicolazione delle informazioni (e l'art. 48 comma 1 affida, inoltre, al Dipartimento per la funzione pubblica il compito di definire schemi standard relativamente alla codificazione e rappresentazione dei dati).

7) Un'attenzione (connessa anche alle predette esigenze di standardizzazione) al problema della qualità delle informazioni diffuse in rete: dei dati diffusi, infatti, le amministrazioni assicurano la qualità (art. 6, comma 1) come integrità, costante aggiornamento, completezza, tempestività, semplicità di consultazione, comprensibilità, omogeneità, facile accessibilità, conformità agli originali, indicazione di provenienza, riutilizzabilità.

8) Un rapporto con la tutela della riservatezza nel quale è la scelta legislativa a definire «*ex ante*» il rapporto tra privacy e conoscibilità (a favore di quest'ultima), e che si sviluppa secondo regole specifiche. Rispetto all'equilibrio che si definisce nel sistema del diritto di accesso, con valutazioni «in concreto» e bilanciamento delle situazioni di fatto, ci troviamo di fronte ad un meccanismo decisamente diverso. Le regole del codice della *privacy* vengono, sostanzialmente, integrate da regole speciali orientate a consentire un regime di conoscibilità «speciale» anche di informazioni e documenti contenenti dati personali. Va detto che il contrasto tra i principi della privacy (finalità del trattamento, divieto di decontestualizzazione, diritto all'oblio) è evidente soprattutto nel quadro dei principi dell'open data, accolti dal decreto, e costituisce uno dei profili più criticati del d.lgs. n. 33 del 2013.

9) La presenza di «politiche» e meccanismi procedurali per la messa a regime di questi elementi conoscitivi «minimi» e la loro implementazione. L'art. 10 del d.lgs. n. 33

prevede, in questo senso, il «Programma triennale per la trasparenza e l'integrità», che ha il compito di definire «l*e misure, i modi e le iniziative volti all'attuazione degli obblighi di pubblicazione previsti dalla normativa vigente, ivi comprese le misure organizzative volte ad assicurare la regolarità e la tempestività dei flussi informativi*». Tra i meccanismi volti a rendere effettive questi obblighi di pubblicità, un ruolo non secondario è giocato dal sistema delle sanzioni, cui sono dedicati in particolare gli articoli 46 e 47 del decreto. Salve alcune sanzioni specifiche (che comminano l'inefficacia di atti, il divieto di nuove provvidenze, sanzioni pecuniarie, ecc.), la violazione degli obblighi di pubblicazione costituisce in via generale «*elemento di valutazione della responsabilità disciplinare*» ed a queste sanzioni soggiace anche il responsabile salvo che provi che l'inadempimento «*è dipeso da causa a lui non imputabile*».

10) Una serie di presidi organizzativi volti a garantire l'effettività di queste misure di conoscenza (l'Anac, già Civit, e gli organismi indipendenti operanti presso ogni amministrazione, secondo quanto previsto in particolare dagli articoli 44 e 45 del d.lgs. n. 33) e di specifiche responsabilità, nonché di apposite professionalità. In questo quadro, un ruolo centrale è rivestito dal «responsabile per la trasparenza» che deve essere individuato in ogni amministrazione ed i cui compiti sono definiti dall'art. 43 del decreto. In particolare, il responsabile «*svolge stabilmente un'attività di controllo sull'adempimento da parte dell'amministrazione degli obblighi di pubblicazione previsti dalla normativa vigente*», con poteri di segnalazione.

4. BIBLIOGRAFIA

Arena G. (2006), *Trasparenza amministrativa*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, Milano, Giuffré, VI, 5954;

Bonomo A. (2012), *Informazione e pubbliche amministrazioni. Dall'accesso ai documenti alla disponibilità delle informazioni*, Bari, Cacucci;

Carloni E. (2005), ed., *Codice dell'amministrazione digitale. Commento al d.lgs. 7 marzo 2005, n. 82*, Rimini, Maggioli;

Carloni E. (2005), *Nuove prospettive della trasparenza amministrativa: dal diritto di accesso alla disponibilità di informazioni*, in *Diritto Pubblic*o, 573;

Carloni E. (2009), *La «casa di vetro» e le riforme. Modelli e paradossi della trasparenza amministrativa*, in *Diritto pubblico*, 779;

Carloni E. (2009), *La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata*, in *Rivista trimestrale di diritto pubblico*, 155;

Carloni E. (2012), *La trasparenza (totale) delle pubbliche amministrazioni come servizio*, in *Munus*, 2012, 179;

Carloni E. (2014), *L'amministrazione aperta. Regole, strumenti, limiti dell'open government*, Rimini, Maggioli;

Carpentieri R. (2013), *L'agenda digitale italiana*, in *Giornale di diritto amministrativo*, 225;

Casetta E., Fracchia F. (2013), *Manuale di diritto amministrativo*, Milano, Giuffré;

Cerrillo Martinez A. (2008), *e-Administraciòn*, Barcelona, Editorial Uoc;

Cerrillo Martinez A. (2011), *The regulation of diffusion of public sector information via electronic means: lessons from the Spanish regulation*, in *Government Information Quarterly*, 28-2, 188;

Cudia C. (2009) *Trasparenza amministrativa e pretesa del cittadino all'informazione*, in *Diritto pubblico*, 99;

Herz M. (2009), *Law lags behind: FOIA and affirmative disclosure of information*, in *Cardozo Public Law, Policy and Ethics Journal,* 585;

Hood C. , Herald D. (2006), ed., *Transparency. The key to better governance?*, Oxford University Press, Oxford;

Lathrop D., L. Ruma (2010), ed., *Open Government: Collaboration, Transparency, and Participation in Practice*, O'Reilly Media, 2010;

Macho R.G. (2010), ed., *Derecho administrativo de la informaciòn y administraciòn transparente*, Madrid, Marcial Pons;

Marzuoli C. (2008), *La trasparenza come diritto civico alla pubblicità*, in Merloni F. et al. (a cura di), *La trasparenza amministrativa*, Milano, Giuffré, 45;

Marzuoli C. (2010), *La transparencia de la administraciòn y el derecho a la informaciòn de los ciudadanos en Italia*, in Macho R.G. (a cura di) (2010), *Derecho administrativo de la informaciòn y administraciòn transparente*, Madrid, Marcial Pons, 151;

Mattarella B.G., Pelissero M. (2013), ed., *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino, Giappichelli;

Merloni F. (2005), ed., *Introduzione all'eGovernment*, Torino, Giappichelli;

Merloni F. (2008), ed., *La trasparenza amministrativa,* Milano, Giuffré, 3;

Merloni F. (2009), *L'eGovernment*, in D'Alessio G., Di Lascio F. (a cura di), *Il sistema amministrativo a dieci anni dalla «Riforma Bassanini»*, Torino, Giappichelli;

Merloni F. (2012), *Istituzioni di diritto amministrativo*, Torino, Giappichelli;

Merloni F. (2013), *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, in Ponti B. (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013 n. 33*, Rimini, Maggioli, 17;

Ponti B. (2008) ed., *Il regime dei dati pubblici*, Rimini, Maggioli;

Ponti B. (2011), *Open Data and Transparency: a Paradigm Shif*, in *Informatica e diritto*, 305;

Ponti B. (2013), ed., *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013 n. 33*, Rimini, Maggioli;

Ponti B. (2013), *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo*, in Ponti B. (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013 n. 33*, Rimini, Maggioli, 75;

Rodotà S. (2009), *Tecnopolitica*,. *La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza;

Savino M. (2013), *Le norme in materia di trasparenza e la loro codificazione*, in B.G. Mattarella, M. Pelissero (a cura di), *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino, Giappichelli, 113;

Savino M. (a cura di) (2010), *The right to open public administrations in europe: emerging legal standards*, OECD, *Sigma Paper*, 46.

IMPLANTACIÓN DE LAS TIC EN LA ADMINISTRACIÓN PÚBLICA: LA PROVINCIA DE GIRONA

Núria Galera
Abogada independiente

Mariona López Ortiz
Abogada independiente

RESUMEN: Nuestra propuesta está basada en el análisis de la evolución e implantación de las TIC en las administraciones públicas. Tomando como ejemplo la provincia de Girona como paradigma de territorio en el que predominan las áreas rurales sobre las áreas urbanas y, a través de datos proporcionados por la Diputación de Girona el Consorcio AOC y otros datos de elaboración propia, detallamos como se han incorporado las TIC en los proyectos y objetivos de los organismos municipales y supramunicipales del territorio en los últimos años. De una parte, se traza la evolución de la e-administración, a través de la incorporación de programas de gestión en los diferentes organismos públicos, así como de las subvenciones otorgadas para la implementación tecnológica. De la otra, se examinan proyectos innovadores en los que las TIC están presentes y que la Diputación de Girona ha llevado a cabo en los últimos años. Se categorizan los proyectos en función de sus objetivos y se analizan a nivel técnico y de repercusión sobre la ciudadanía. Entre los proyectos analizados destacan: i) las E-RUTAS: un sistema de guía por GPS que interpreta, en lenguaje multimedia, el patrimonio de las vías verdes; ii) el Sistema de Información Municipal (SIMPSAP), a través del cual los ayuntamientos se adhieren al uso de programas de soporte en materia de salud pública; y iii) el proyecto «Girona territori cardioprotegit», que gestiona la red de desfibriladores instalados en la vía pública más extensa de Europa.

PALABRAS CLAVE: Administración electrónica, áreas rurales, sitios web, información pública, servicios electrónicos.

1. INTRODUCCIÓN

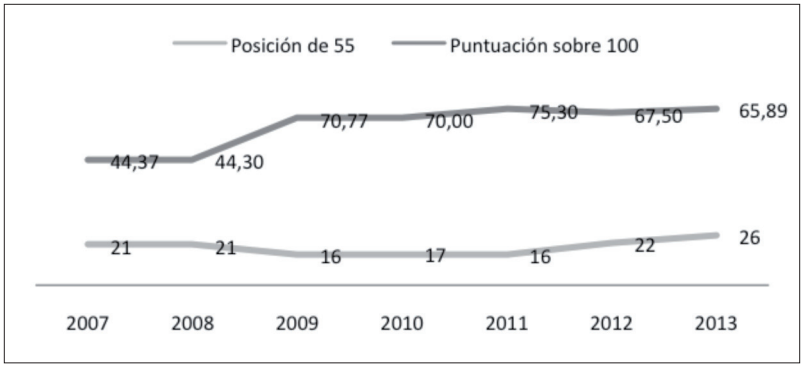
El auge de las tecnologías de la información y la comunicación ha comportado que, en las últimas décadas, los gobiernos de todo el mundo hayan adaptado su forma de operar, incorporando el enorme potencial de estas tecnologías para aumentar la eficacia y eficiencia de la administración pública mediante nuevas vías de interacción con los ciudadanos, las empresas y organizaciones, dando lugar a la administración electrónica o e-administración. Con la ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos[1]

1 Disponible en : http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

y la ley 29/2010, de 3 de agosto del uso de los medios electrónicos en el sector público de Catalunya, se reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas a través de medios electrónicos, lo que implica una obligación correlativa a dichas Administraciones que deben poner los medios para que el ciudadano pueda ejercer su derecho. En la última década los gobiernos supramunicipales han realizado numerosas acciones encaminadas a facilitar el cambio de la administración tradicional a la e-administración: se han creado organismos y o áreas específicos como el Consorci d'Administració Oberta de Catalunya (Consorcio AOC)[2] y el área de Régimen Económico y Nuevas Tecnologías de la Diputación de Girona, invertido capital, concedido subvenciones, creado software específico, impulsado y realizado estudios sobre el tema, etc.

Entre otros factores, estas iniciativas han situado al Estado español en la tercera posición entre los líderes emergentes en desarrollo de la e-administración según datos de la e-Government Survey 2012 realizada por la ONU. Este dato se ve apoyado por el ranquin de la Waseda University, que puntúa diferentes indicadores en 55 países, siendo los más desarrollados Singapur y Estados Unidos en las primeras posiciones y los menos Irán y Uzbekistán que ocupan los lugares 54 y 55 en la lista. Según esta encuesta la e-administración en el Estado español se encuentra en un nivel de desarrollo medio-alto.

Gráfica 1. Evolución del Estado español en el ranquin internacional de e-administración



Fuente: datos de la Waseda University Institute of e-Government [3].

2 Entidad existente des del 2001 que tiene la finalidad de colaborar con la Generalitat y los entes locales y prestar todo tipo de asistencia en aspectos relacionados con la e-administración. Más información en: http://www.aoc.cat/Inici/CONSORCI-AOC/Que-es-el-Consorci-AOC (último acceso 07/03/2014).

3 Gráfico de elaboración propia a partir de los datos de los ránquines que la Waseda University Institute of e-Government realiza anualmente, valorando una serie de indicadores que marcan el desarrollo de la e-administración de 55 países.

El presente artículo se limita territorialmente a la provincia de Girona, formada por 221 municipios y que se caracteriza por el predominio de áreas rurales y núcleos urbanos pequeños. La tabla 1 muestra cómo se distribuye la población y cabe destacar que el 84,6% de los municipios son menores de 5.001 habitantes y concentran el 24% de la población.

Tabla 1. Distribución de los municipios y habitantes de la provincia de Girona por tramos de población (2013)

Tramos de población	Municipios	Habitantes	Porcentaje de habitantes	Porcentaje acumulado de habitantes
Hasta 500 hab.	86	23.329	3%	3%
501 a 1.000 hab.	44	32.023	4%	7%
1.001 a 5.000 hab.	57	128.806	17%	24%
5.001 a 10.000 hab.	15	99.193	13%	37%
10.001 a 30.000 hab.	13	191.175	25%	62%
Más de 30.000 hab.	6	287.106	38%	100%
Total	221	761.632	100%	

Fuente: elaboración propia[4].

Con los datos que se exponen en los siguientes puntos se pretende, en primer lugar, trazar la evolución de la e-administración a través de las subvenciones otorgadas para la implementación tecnológica desde 2005 y hasta 2014, así como la incorporación de programas de gestión en los diferentes organismos públicos y, en segundo lugar, examinar proyectos innovadores en los que las TIC están presentes y que la Diputación de Girona ha llevado a cabo en los últimos años.

2. IMPLANTACIÓN DE LAS TIC EN EL ÁMBITO MUNICIPAL

Para poder determinar el marco tecnológico existente y la evolución en la implantación de la e-administración en la provincia de Girona es importante por un lado, conocer la respuesta ante las iniciativas para la instalación y desarrollo de programas informáticos y otras herramientas, que suponen servicios directos al ciudadano o bien mejoras en la gestión municipal y por otro lado, conocer el destino de la inversión efectuada en los últimos años.

Las Administraciones Públicas supramunicipales que actúan como agentes relevantes en la implantación de la e-Administración en los municipios catalanes son: la

4 Tabla de elaboración propia con datos del Instituto Nacional de Estadística (INE) extraídos del padrón a fecha 1 de enero de 2013.

Generalitat de Catalunya con el Consorcio AOC de un lado y las Diputaciones provinciales del otro. Para este estudio trataremos mayoritariamente datos de la Diputación de Girona[5], por ser esta la que tradicionalmente actúa más directamente sobre el territorio, y porque la política de colaboración entre administraciones, comporta que parte de la ejecución de proyectos conjuntos haya recaído habitualmente sobre este órgano.

2.1. Páginas web municipales

Uno de los pilares de la e-administración es la existencia de sitios web con información básica sobre la institución. Autores como Baum y Di Miao (2000), Hiller y Bélanguer (2001), Moon (2002), Siau Long (2005), Layne y Lee (2001) [6] consideran la puesta a disposición de información al ciudadano como el primer nivel en la implantación de la e-administración.

Actualmente en la provincia de Girona los 221 municipios cuentan con páginas web activas. En la tabla 2 se muestra la evolución en la prestación del servicio que ofrece la Diputación de Girona para la creación y mantenimiento del 65,6 % de estas webs. Así, en los últimos 10 años, se han creado 145 webs dando servicio a 143 municipios[7]. El grueso de los sitios web (75) se crearon en 2003 coincidiendo con el inicio de la campaña y el servicio se ha dirigido a municipios de menos de 5.000 habitantes con dos excepciones, en que los municipios contaban con 5.356 y 5.314 habitantes en el año de la prestación. La Diputación anunció el 31 de enero que en el transcurso del 2014 se procederá a renovar 140 webs de municipios de menos de 5.000 habitantes[8]. Esta renovación incluye, entre otras cosas, el cambio del soporte SharePoint actual a WordPress. No se muestran datos de los años de creación de los sitios web en los municipios mayores de 5.000 habitantes aunque se ha comprobado[9] que todos tienen sitio web activo.

Tabla 2. Inicio de prestación del servicio de creación de páginas web por municipios

Año	Hasta 500 hab.	501 a 1.000 hab.	1001 a 5.000 hab.	5.001 a 10.000 hab	Total
2003	67	26	24	0	117
2005	1	0	0	1[10]	2
2006	0	0	1	0	1

5 Facilitados por el departamento de Sistemas y Tecnologías de la Información.

6 Todos estos autores proponen diferentes sistemas para medir la implantación de la e-administración basados en niveles que van del uno al cuatro o al cinco en función de sistema.

7 Los municipios de Sils y Quart han solicitado dos veces el servicio.

8 La noticia se puede consultar en: http://www.ddgi.cat/web/noticia.seam?nivellId=244&dataModelSelection=&noticiaId=2715&cid=71528&categoriaId=7 (último acceso 28/02/2014).

9 A fecha 20/02/2014 se realizó una búsqueda específica de las webs oficiales de los municipios en la provincia de Girona.

Año	Hasta 500 hab.	501 a 1.000 hab.	1001 a 5.000 hab.	5.001 a 10.000 hab	Total
2007	0	1	1	0	2
2008	3	2	1	1	7
2009	3	2	2	0	7
2010	1	0	1	1	3
2011	0	1	2	0	3
2012	0	1	0	0	1
2013	0	0	2	0	2
Total	75	33	34	3	145

Fuente: elaboración propia[11].

a) Sede electrónica

Las webs municipales cumplen con funciones de carácter informativo, pero también permiten la interacción con el ciudadano brindándole la posibilidad de realizar trámites en línea a través de identificación digital. En este sentido, existe un módulo de gestión municipal ofrecido por el Consorcio AOC llamado e-TRAM[12] que facilita a los ayuntamientos la prestación de hasta 40 trámites diferentes online tales como: presentación de instancias, domiciliación de tributos, y certificados de empadronamiento, entre otros. Aunque no ofrecen todos los trámites posibles, este servicio lo tienen visible en la web el 76,5 %[13] del total de los municipios y el 83 % si se atiende solo a los mayores de 1000 habitantes. Otro servicio ofrecido por el Consorcio AOC que facilita a los municipios la implantación de una sede electrónica es el SEU-e[14], este servicio lo utilizan 21 municipios[15] de la demarcación (el 9,5%) y se puede disfrutar simultáneamente con el e-TRAM. Autores como Hiller y Bélanger (2001), Layne y Lee (2001) y Siau Long (2005) consideran la interacción y transacción administración-ciudadano, en que se pueden realizar trámites completos online, como la asunción del segundo y el tercer nivel en la incorporación de la e-administración.

10 Según datos del INE este municipio contaba con 3.947 habitantes en el año 2005.

11 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

12 Se pueden consultar las características del e-TRAM en: http://www.aoc.cat/Inici/SERVEIS/Relacions-amb-la-ciutadania/e-TRAM (último acceso el 20/02/2014).

13 Datos extraídos a partir de listado de municipios publicado por el Consorcio AOC con fecha 13 de setiembre de 2013.

14 Se pueden consultar las características del SEU-e en: http://www.aoc.cat/Inici/SERVEIS/Relacions-amb-la-ciutadania/SEU-e (último acceso el 20/02/2014).

15 Datos extraídos a partir de listado de municipios publicado por el Consorcio AOC con fecha febrero de 2014.

Es destacable el hecho de que la identificación digital se convierta en un elemento imprescindible para acceder a los trámites online, incluso para aquellos trámites que presencialmente no precisan de la identificación de la persona que realiza el registro de entrada.

b) Tablón electrónico

La ley 11/2007 de 22 de junio en su artículo 12 considera que los actos y comunicaciones que deban publicarse en el tablón de anuncios se podrán publicar substituyendo o complementando al tablón en la sede electrónica del organismo correspondiente. Al respecto, el Consorcio AOC ofrece el servicio e-TAULER[16] a aquellos municipios que quieran incorporarlo en su sede electrónica.

Tabla 3. Prestación del servicio de e-TAULER por municipios.

Tramos de población	Instalado	No instalado	Total
Hasta 500 hab.	4	82	86
501 a 1.000 hab.	2	42	44
1.001 a 5.000 hab.	10	47	57
5.001 a 10.000 hab.	2	13	15
10.001 a 30.000 hab.	5	8	13
Más de 30.000 hab.	4	2	6
Total	27	194	221

Fuente: elaboración propia[17].

2.2. Programas informáticos y otras herramientas

Un indicador importante para conocer el grado de incorporación de la e-administración es conocer las herramientas tecnológicas de gestión interna utilizadas por los municipios. Según Coursey y Norris (2008) estas herramientas son claves para el cambio de paradigma en la estructura de la administración, que debe transmutar la estructura vertical clásica hacia una estructura más horizontal propia de la e-administración.

2.2.1. Gestor de expedientes

La incorporación de un gestor de expedientes es un cambio relevante en el funcionamiento de una institución, experiencias como las relatadas por Gil-García y Pardo

16 Se pueden consultar las características del SEU-e en: http://www.aoc.cat/Inici/SERVEIS/Relacions-amb-la-ciutadania/e-TAULER (último acceso el 20/02/2014).

17 Datos extraídos a partir del listado de municipios publicado por el Consorcio AOC con fecha febrero de 2014.

(2005) apuntan a la importancia de tener capacidad de gestión para grandes volúmenes de información, como un elemento que afecta directamente a la mejora en la eficiencia y la eficacia del funcionamiento de las instituciones.

Desde el año 2010 los ayuntamientos de Girona pueden acceder a un servicio de gestor de expedientes[18] ofrecido por la Diputación. Hasta la fecha se han acogido al servicio 65 municipios (29,4 % del total)

Tabla 4. Inicio de prestación del servicio de gestor de expedientes por municipios.

Tramos de población	2010	2011	2012	2013	Total
Hasta 500 hab.	5	10	3	1	19
501 a 1.000 hab.	4	3	3	4	14
1.001 a 5.000 hab.	9	7	5	1	22
5.001 a 10.000 hab.	3	2	3	0	8
10.001 a 30.000 hab.	2	0	0	0	2
Total	23	22	14	6	65

Fuente: elaboración propia[19].

La acogida de este programa responde principalmente a dos factores relacionados con el tamaño del municipio, ya que los municipios más grandes llevan años utilizando gestor de expedientes y en lo referente a los municipios más pequeños son menos receptivos a realizar cambios en la operativa habitual y no se entiende el gestor de expedientes como una necesidad.

Para facilitar la transición de los municipios de menos de 5.000 habitantes a la operativa con gestor de expedientes y garantizar así el éxito de la migración, la Diputación de Girona y el Consorcio AOC han iniciado un proyecto piloto llamado e-SET[20]. Este proyecto consiste en poner en funcionamiento un sistema de trabajo que opera en todo el ayuntamiento, previo a la instalación del software. Se modifican patrones de conducta y de funcionamiento, incorporando estructuras y estándares que implican la familiarización del personal con los protocolos, antes incluso de instalar el software en los sistemas informáticos.

2.2.2. Padrón municipal de habitantes

Una gestión eficaz del padrón municipal de habitantes supone una gestión eficaz de la población y del territorio, y se trata de uno de los servicios que se han beneficiado de

18 Se trata del gestor de expedientes ABSIS.

19 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

20 Actualmente en funcionamiento en 4 municipios (La Vall de Bianya, La Cellera de Ter, Riudellots de la Selva, Fornells de la Selva).

la informatización con mayor prontitud, de hecho, es el servicio más antiguo de los que ofrece la Diputación a los municipios. En la tabla 4 se muestra la evolución de las peticiones del servicio, en la actualidad 126 de los 187 municipios de hasta 5.000 habitantes se han adherido al plan provincial de gestión del padrón municipal[21].

Tabla 5. Inicio de prestación del servicio de padrón municipal por municipios y tramos de población

Año	Hasta 500 hab.	501 a 1.000 hab.	1001 a 5.000 hab.	5.001 a 10.000 hab.	10.001 a 30.000 hab.	Total
1999	1	1	2	0	0	4
2000	19	3	5	1	0	28
2001	5	1	1	0	0	7
2002	5	1	1	0	0	7
2003	1	1	0	0	0	2
2004	1	0	2	1	0	4
2005	2	2	5	2	0	11
2006	3	1	5	1	0	10
2007	1	3	3	0	0	7
2008	3	2	3	2	0	10
2009	3	4	3	1	0	11
2010	6	3	3	0	1	13
2011	6	1	2	0	1	10
2012	2	5	1	0	0	8
2013	1	0	3	2	0	6
Total	59	28	39	10	2	138

Fuente: elaboración propia[22].

2.2.3. Registro de entrada y salida

Los registros de entrada y salida cumplen funciones de gestión interna, aumentan la seguridad y pueden interactuar con otras herramientas como los gestores de expedientes o los tramitadores online y también pueden enlazar con otros sistemas de información de conectores estándar. La Diputación de Girona ofrece este servicio desde el año

21 El servicio se presta a través de la aplicación UNIT4, los ayuntamientos tienen el control con los accesos y permisos pertinentes, pero la carga tecnológica de mantenimiento y copias de respaldo recae sobre la Diputación.

22 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

2010 en colaboración con el Consorcio AOC y utilizando el sistema ERES[23], la tabla 6 muestra que la implantación de este servicio aún no está generalizada.

Tabla 6. Inicio de prestación del servicio de registro electrónico por municipios.

Tramos de población	2010	2011	2012	2013	Total
Hasta 500 hab.	9	25	2	3	39
501 a 1.000 hab.	8	3	7	7	25
1.001 a 5.000 hab.	7	12	9	2	30
5.001 a 10.000 hab.	1	1	2	2	6
10.001 a 30.000 hab.	1	1	0	0	2
Total	26	42	20	14	102

Fuente: elaboración propia[24].

2.3. Maquinaria y sistemas informáticos

Tan importante como tener los programas y servicios adecuados, es tener la maquinaria y los sistemas informáticos que permitan el correcto funcionamiento de estos. En cualquier entidad compleja es necesaria una renovación y mantenimiento constante para sacar el máximo partido a los equipos y redes, ya que con los cambios tecnológicos la maquinaria puede quedar obsoleta con facilidad.

Un indicador que puede acercarnos a la calidad y estado de los sistemas informáticos de los municipios de Girona es la inversión económica que se ha realizado en los últimos años. No disponemos de los recursos que han destinado los propios municipios directamente, pero sí de las subvenciones que han recibido de la Diputación de Girona. La Diputación, lleva años otorgando ayudas destinadas a tres bloques: la mejora de material informático, la mejora de las redes informáticas y la mejora de software. Las ayudas se otorgan, bien mediante convocatoria en la que concurren los ayuntamientos y otras entidades, o bien por adjudicación directa, cuando se trata de una dificultad sobrevenida o de un objeto o sujeto exento de la convocatoria pero que se estima adecuado para recibir la ayuda.

La tabla 7 muestra los totales de las inversiones realizadas a los ayuntamientos de 2005 a 2014, sin distinguir entre las subvenciones que responden a las convocatorias y las que responden a adjudicaciones directas. Cabe destacar que el presupuesto destinado a estas inversiones ha bajado considerablemente desde 2011.

23 Se pueden consultar las características del ERES en: http://www.aoc.cat/Inici/SERVEIS/Gestio-interna/ERES-Registre-d-entrada-i-sortida (último acceso el 20/02/2014).

24 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

Tabla 7. Inversión en euros a los municipios por tramos de población

Año	Hasta 500 hab.	501 a 1.000 hab.	1001 a 5.000 hab.	5.001 a 10.000 hab.	10.001 a 30.000 hab.	Más de 30.000 hab.	Total
2005	104.563,65	109.880,59	236.773,12	64.782,00	36.000,00	24.000,00	575.999,36
2006	160.269,51	108.168,24	228.257,85	72.855,09	76.000,00	25.755,50	671.306,19
2007	100.780,61	96.432,99	234.530,41	112.225,17	138.431,71	123.805,00	806.205,89
2008	119.073,03	67.410,80	124.781,94	127.666,29	158.369,88	189.620,00	786.921,94
2009	116.411,90	69.002,52	111.074,98	133.414,10	235.130,77	112.487,21	777.521,48
2010	132.531,24	68.197,13	107.928,63	70.458,85	192.639,65	40.800,00	612.555,50
2011	95.991,65	65.808,32	85.330,13	70.451,00	68.000,00	52.000,00	437.581,10
2012	94.276,52	49.701,48	93.701,16	31.539,28	30.756,73	21.494,28	321.469,45
2013	39.223,89	27.879,06	82.114,03	44.435,37	91.350,68	48.000,00	333.003,03
2014[25]	59.271,17	39.655,36	93.274,39	50.163,56	86.635,50	69.000,00	397.999,98
Total	1.022.393,17	702.136,49	1.397.766,64	777.990,71	1.113.314,92	706.961,99	5.720.563,92

Fuente: elaboración propia[26]

Analizando los datos por municipios, se detecta una repartición con valores extremos que derivan en una desviación significativa entre la media y la mediana. Estos valores máximos extremos puntualmente llegan a triplicar el máximo que se puede conseguir por medio de convocatoria y no responden a criterios de población. En referencia a los valores mínimos estos pueden responder a una falta de concurrencia a las convocatorias por parte del órgano municipal.

Tabla 8. Inversión máxima y mínima en euros realizada por municipios de 2005 a 2014

Tramos de población	Inversión máxima por municipio	Inversión mínima por municipio	Inversión por municipio (media)	Inversión por municipio (mediana)	Inversión media por habitante
Hasta 500 hab.	34.265,08	907,00	11.888,29	10.516,20	43,82
501 a 1.000 hab.	35.498,66	4.348,47	15.957,65	14.804,62	21,93
1.001 a 5.000 hab.	80.208,75	4.500,27	24.522,22	22.404,89	10,85
5.001 a 10.000 hab.	122.375,44	7.224,88	51.866,05	38.237,77	7,84
10.001 a 30.000 hab.	184.149,05	20.676,52	85.639,61	67.817,08	5,82
Más de 30.000 hab.	176.153,69	15.370,13	117.827,00	109.686,71	2,46

Fuente: elaboración propia[27]

25 Los datos de 2014 son provisionales, pueden variar a lo largo del año en función de las adjudicaciones directas.

26 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

27 Tabla elaborada a partir de datos facilitados por la Diputación de Girona.

Si comparamos el tamaño poblacional con el importe de las subvenciones recibidas de la Diputación, se detecta que existe una correlación entre tramos de población y la inversión media. De igual forma, existe correlación entre los tramos de población y la inversión media por habitante. En el primer caso la relación es positiva y en el segundo la relación es negativa. Es decir, cuanto mayor es el número de habitantes del municipio, mayor es la inversión total (la relación es directamente proporcional). En cambio, si se toma como referencia la media por habitante, a mayor número de habitantes menor media de inversión (relación inversamente proporcional).

Finalmente, y para tener una fotografía global de la demarcación, de media la población se sitúa en los 3.446,30 habitantes por municipio, y la inversión media por municipio es de 23.866,80 €.

2.4. Conclusiones

Para valorar el estado de la incorporación de la e-administración, se han tenido en cuenta los niveles de Layne y Lee (2001)[28] sobre otras escalas y niveles aplicables[29]. Según estos niveles, la provincia de Girona tendría plenamente asumido el primer nivel, al ofrecer todos sus municipios información básica online, el segundo nivel lo tendrían asumido el 76,5 % de los municipios, ya que permiten a los ciudadanos interactuar con la administración online y realizar trámites sencillos. El nivel 3 supone automatizar procesos e integrar funciones de administraciones diferentes la asunción de este nivel, aún en proceso, depende de las iniciativas de servicios que ofrecen los organismos supramunicipales como la diputación de Girona y el Consorcio AOC. El último nivel responde al concepto de «ventanilla única» y se trataría de un solo portal de acceso a la administración que ofreciera todos los trámites posibles al ciudadano. Al margen del grado de implantación de la e-administración es importante el grado de uso que se tenga por parte del ciudadano, sobre esto influyen múltiples factores como la dificultad técnica, la visibilidad, el acceso a recursos informáticos, la homogeneidad en la estructura de la información, y factores sociales directamente relacionados con el usuario.

La identificación mediante firma o certificado digital es una carga para el ciudadano que realiza trámites online. Esta obligación establecida por la ley supone una imposición

28 El sistema de Layne y Lee es el siguiente: nivel 1 información: acceso a información estática o básica a través de sitios web; nivel 2 Transacción: se aumenta la variedad de información que se ofrece y se permite a los ciudadanos realizar operaciones sencillas online, como rellenar formularios; nivel 3 Integración vertical: esta fase supone el inicio de la transformación de los servicios de la administración automatizando procesos existentes. Se centra en integrar funciones de administraciones a diferentes niveles; nivel 4 Integración horizontal: integrar diferentes funciones de sistemas separados para ofrecer a los usuarios un servicio unificado.

29 Como los desarrollados por Australian National Auditing Office, (1999) y Hiller, J.; Bélanger, F. (2001).

sobre el ciudadano a diferencia de aquel que realiza el trámite de manera presencial y que puede hacerlo sin identificarse. El trámite online exige más garantías que el presencial, cosa que se puede convertir en un inconveniente para la implantación de la e-administración.

Es básico que los servicios se presten desde entidades supramunicipales que asumen la carga tecnológica y realizan el mantenimiento y las actualizaciones necesarias, de esta manera se garantiza el uso de conectores estándar, y una homogeneidad necesaria en los servicios y sistemas que facilita el enlace con los sistemas de información de otras corporaciones, pero sobre todo se permite a los municipios con recursos limitados implementar proyectos que tecnológicamente y económicamente están muy por encima de sus posibilidades.

La continuidad y el aumento en los servicios que ofrece la Diputación de Girona, a pesar de la crisis económica, indica una apuesta por este tipo de prestación de servicios, especialmente en relación con la importante reducción en materia de subvenciones que ha realizado este organismo.

La existencia de desigualdades y casos con valores extremos en la repartición de subvenciones, invita a un análisis más profundo de estos casos puntuales, en que se consideren criterios de repartición diferentes al meramente poblacional añadiendo factores políticos y económicos. A pesar de estas desviaciones de los datos analizados se puede concluir que la inversión en un municipio está relacionada con el número de habitantes, y que se aplica un factor que se podría llamar «equilibrio territorial» que hace que la inversión por habitante sea mayor cuanto más pequeño sea el municipio des de un punto de vista poblacional. Des de una visión de análisis de políticas públicas, esta opción se justifica, si tenemos en cuenta que la capacidad de los municipios pequeños para implementar acciones en materia de nuevas tecnologías es más limitada.

3. APUESTAS SUPRAMUNICIPALES POR EL USO DE LAS TIC

3.1. Una aplicación para las Vía Verdes

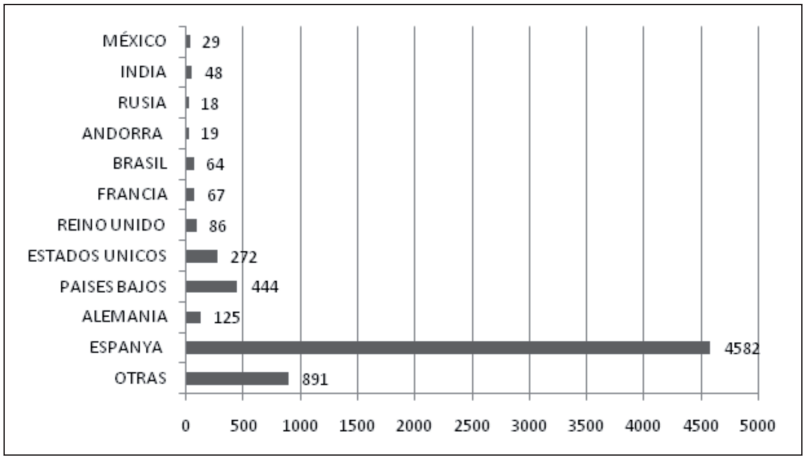
Las vías verdes de la demarcación de Girona, están formadas por cuatro rutas, que entre todas ellas suman un recorrido de aproximadamente 117 kms, junto con algún ramal que va des de los Pirineos hasta la Costa Brava. Históricamente estos recorridos eran los que configuraban la red de ferrocarril de vía estrecha («carrilet») que unían las diferentes poblaciones de la provincia. Gracias a su recuperación y mantenimiento se pude disfrutar de la riqueza cultural y del entorno de estas comarcas, ya sea andando o en bicicleta.

El concepto clave de la inclusión de la e-administración en la gestión de estas rutas verdes entra en juego con la aplicación para móvil de las E-Rutas, creado por el «Consorci de les Vies Verdes» de la Diputación de Girona, este sistema pone al alcance de los ciudadanos unos itinerarios multimedia guiados por GPS que permiten descubrir e interpretar los secretos del territorio. La Guía el visitante que realiza la vía verde con un sistema GPS da un lugar a otro a través de un itinerario prefijado. Interpreta el patrimo-

nio natural, arquitectónico y paisajístico que se encuentra en estos itinerarios a medida que el usuario va avanzando en la ruta.

La aplicación E-Rutas para teléfono móvil está disponible en todos los sistemas operativos, y según datos oficiales, se observa un índice de descargas positivo aunque con posibilidades de aumentar a plazo corto si se implantan las medidas dinamizadoras oportunas. Destaca la diversidad de países des de los que se descarga la aplicación y el interés que suscita.

Gráfica 2. Índice de descargas en Google Play según país a fecha 21 de febrero de 2014



Fuente: Consorci de les Vies Verdes

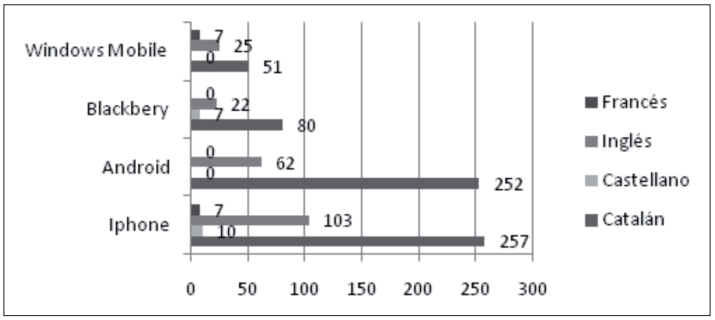
A su vez, las vías verdes se integra dentro del Sistema de Información Geográfica que se encarga de inventariar y georeferenciar el mobiliario urbano (bancos, papeleras, rótulos, etc.). El sistema permite asociar formularios de incidencias que contienen información de cada elemento (fecha de colocación, fabricante, fecha de reparación etc). La información que puede ser de interés para los usuarios se vuelca en un vuelo virtual 3D. Así mismo, permite controlar de forma exhaustiva cualquier incidencia. Así por ejemplo, en caso que haya un banco roto o en mal estado el sistema permite monitorizar el momento en que se detectó este incidencia, quien la detectó, el lugar exacto donde se encentra este elemento, el instante en el cual se dio la orden de reparo y el tiempo que precisó. Todo ello a lo largo de los 117 km de la red para los diferentes elementos de la misma.

La página web del Consorcio de las Vías Verdes, contiene información sobre las vías en cuatro idiomas (catalán, castellano, inglés y francés). Está organizada en seis apartados: 1) Rutas: informa detalladamente sobre las cuatro rutas; 2) Servicios Turísticos: facilita información complementaria al usuario sobre alojamientos, restaurantes, agencias de viajes, alquiler de vehículos, etc; 3) Noticias media: ofrece enlaces con la

aplicación de las e-rutas, fotografías, vídeos, mapas opiniones de los usuarios, descuentos y promociones; 4) El consorcio: ofrece información institucional y jurídica sobre el ente; 5) Tienda: enlaza con actividades y productos complementarios, permite adquirir productos de «merchandising; 6) Notificación de incidencias/mejoras: permite que los usuarios de las vías informen de cualquier incidencia que hayan detectado en la red a la vez que se informa de posibles incidencias (obras, etc.).

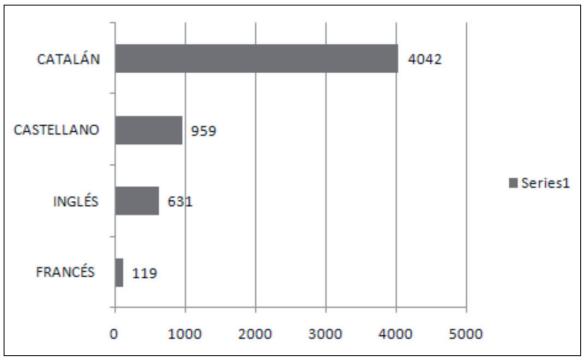
Referente al índice de visitas a la web se observa una evolución creciente a medida que transcurre el tiempo, tanto en el acceso des de teléfono móvil como en el acceso des de la web. Síntoma inequívoco que la implantación de este sistema suscita interés a los ciudadanos que se convierte con el tiempo en usuarios de las vías verdes.

Gráfica 3. Índice de visitas a la web E-RUTAS según sistema operativo móvil durante el período comprendido entre 1 de noviembre de 2010 a 20 de febrero de 2014.



Fuente: Consorci de les Vies Verdes

Gráfica 4. Índice de visitas a la web E-RUTAS durante el período comprendido entre 1 de noviembre de 2010 a 20 de febrero de 2014.



Fuente: Consorci de les Vies Verdes

3.2. SIMSAP

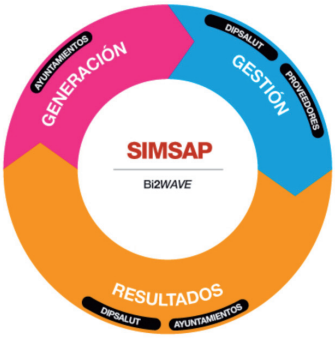
Uno de los avances de la e-administración es la implantación de diferentes programas para mejorar la relación interadministrativa, con la finalidad de hacer más proactivo el servicio al ciudadano. En este sentido, se han creado plataformas que permiten a ambas administraciones interactuar de manera simultánea, creando a su vez un registro de datos que generan un recurso futuro.

El Sistema de Información Municipal en Salud Pública (SIMSAP), es la plataforma que utilizan los ayuntamientos de la demarcación de Girona para interactuar con «Dipsalut» (Organisme Autònom de Salut Pública de la Diputació de Girona), en materia de salud pública municipal. Esta plataforma permite una comunicación ágil entre ambos. Consiste en una aplicación web a la que tienen acceso: Dipsalut, los ayuntamientos y los proveedores que realizan el servicio en concreto. De esta manera entre ellos se intercambian datos, de los programas de protección y promoción de la salud en concreto, y se gestionan las solicitudes de servicio de estos programas.

SIMSAP, se presenta finales del año 2010 como una solución de gestión para la salud pública municipal, basado en el concepto de «Cloud computing», mediante el cual se tienen acceso a unos datos centralizados, de manera segura y dimensional.

La simplicidad del uso y los requisitos de acceso hacen que SIMSAP sea una herramienta muy accesible, de manera que el único requisito es tener acceso a un ordenador con conexión a internet. Cada ayuntamiento dispone de cuatro perfiles con diferentes permisos (gestores, revisores, consultores y editores), de esta manera se pueden consultar y gestionar todas las solicitudes y desarrollo de los programas con impacto en el municipio.

Figura 1. Realidad de los actores implicados en la plataforma, según la fase de evolución de las solicitudes.



Fuente: Dipsalut

Este programa pone a disposición de todos los actores el detalle de todas las actuaciones que se están llevando a cabo en materia de salud pública en un territorio concre-

to, así como consultar los resultados dimanantes de estas actuaciones, creando de esta manera una base de datos actualizada, pudiendo el municipio realizar un histórico de actuaciones, resultados y solicitudes.

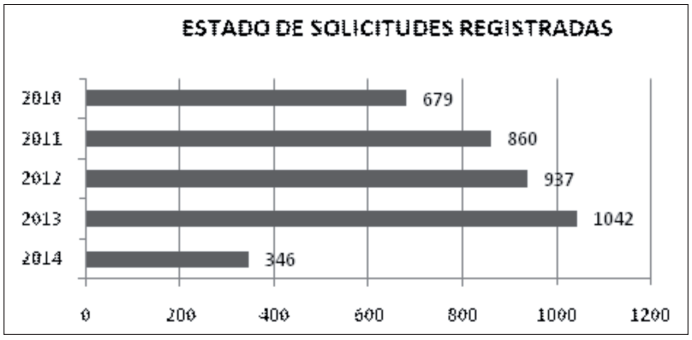
Una de las funcionalidades a destacar del SIMPAP, es la Georeferenciación, a través de esta funcionalidad, los municipios pueden visualizar sobre el mapa de su municipio todos los equipamientos sobre los que se está llevando a cabo alguna actuación.

Los proveedores de los servicios de salud pública, juegan un papel importante en el desarrollo de la relación Dipsalut-Ayuntamiento, ya que SIMSAP les permite tener en un único programa toda la información de los programas que han realizado, siendo un canal de comunicación eficaz y efectivo con el organismo y el ayuntamiento.

SIMSAP, representa una herramienta que permite alimentar los indicadores y poder monitorizar la actividad y analizar los resultados para poder obtener una visión completa de la realidad e cada municipio y de la demarcación. Todo ello permite adaptar los programas y los servicios a las necesidades del territorio y optimizar el desarrollo de las decisiones en salud pública municipal.

Según datos proporcionados por Dipsalut, des de la puesta en funcionamiento del programa, los ayuntamientos de la demarcación de Girona han realizado más de 5.000 solicitudes de programas del Catalogo de Servicios, con aproximadamente 30.000 actuaciones sobre los municipios, en más de 3.500 instalaciones municipales geolocalizadas sobre el mapa de cada localidad.

Gráfica 5. Índice de de estado de solicitudes registradas des del año 2010 hasta el mes de enero de 2014.



Fuente: datos Dispalut

En entrevistas con el Ayuntamiento de Girona, podemos comprobar la accesibilidad de los municipios a esta plataforma y la sencillez de uso de la misma. Generalmente, nos transmiten un nivel de satisfacción mediano-alto con la implementación de este sistema. Al acceder a la plataforma nos encontramos con un menú deducible, con indicaciones claras y una estructura definida.

3.3. Territorio cardioprotegido

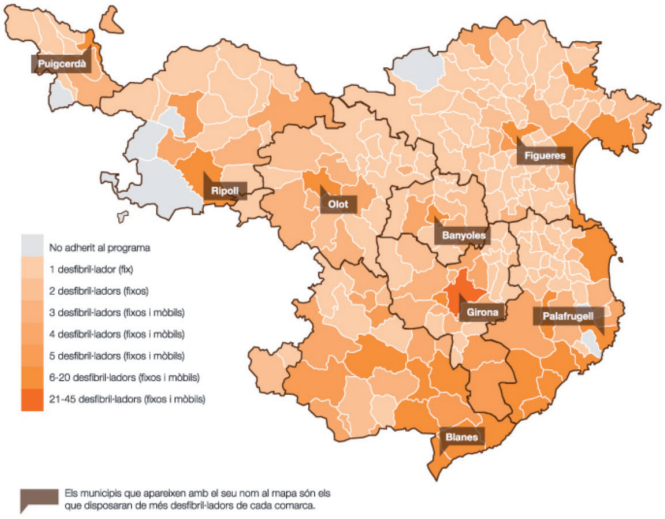
El «Girona, territorio cardioprotegido»[30] es la sinergia entre la preocupación por la prevención y protección de la salud de los ciudadanos y la implantación de la e-administración en un contorno municipal. Se pone al alcance de los ciudadanos una red de desfibriladores públicos para que hagan un uso de estos en casos de emergencia médica. No obstante, lo importante y el gran avance que supone esta red pública, es la implantación en 214 municipios de los 221 de la demarcación de Girona, de como mínimo un desfibrilador disponible y al alcance de todo el mundo. Según datos de Dipsalut, esta cifra supone una adhesión del 97% de los municipios de la demarcación. Se encuentran a disposición de los ciudadanos un total de 500 desfibriladores fijos y 130 de móviles. A través de la web de Dipsalut el ciudadano puede consultar la ubicación de los desfibriladores mediante un mapa interactivo que informa de la ubicación exacta de los desfibriladores en cada municipio.

Nos encontramos ante un servicio que se ofrece a los ciudadanos, una nueva manera de entender la gestión de la salud pública, que en un principio debe tratar de ser más accesible y sencilla al uso para los ciudadanos y, práctica y sostenible para la administración. La puesta en marcha de este tipo de proyectos supone una apuesta de la e-administración hacia la proximidad con el ciudadano, y es la prueba exacta de si los canales de propagación utilizados son efectivos. Hace unos años, seria inimaginable que ninguna Diputación desplegara una red pública de desfibriladores y que el principal canal de propagación fuera electrónico.

Seguramente, no transcurrirá demasiado tiempo para que esta red esté disponible en aplicación para teléfono móvil, en versión app, mediante el cual los ciudadanos puedan consultar en todo momento, independientemente de la población donde estén, la situación de todos los desfibriladores.

30 El «Girona, territorio cardioprotegit», es el proyecto de desfibrilación pública más grande de Europa, siendo la demarcación de Girona, el territorio cardioprotegido más grande de la Unión Europea.

Figura 2. Distribución territorial de los desfibriladores.



Fuente: Dipsalut[31]

3.4. Conclusiones

En este recorrido por las apuestas municipales por el uso de las TIC, realmente es mucha la información que constata que cada vez es más frecuente la utilización de estas herramientas por parte de las administraciones para interaccionar con los ciudadanos. Todo ello conlleva una adaptación natural de los ciudadanos y a un cambio en las relaciones con la administración.

Es imprescindible reflexionar sobre la sostenibilidad y el mantenimiento de este tipo de plataformas para hacerlas eficientes y que generen ahorro en un futuro. Generalmente la puesta en funcionamiento de las TIC, supone una inversión económica inicial y una inversión especial de aprendizaje y tiempo por otra parte, tanto del personal de las administraciones públicas como para los ciudadanos. Es entonces de esperar una preocupación por parte de las administraciones públicas por tratar de mantener este tipo de servicio de gestión y así optimizar al máximo su funcionamiento.

Si trazásemos un gráfico de la evolución de las TIC en las administraciones públicas en la última década sin duda sería un gráfico con evolución positiva, donde los diferentes actores implicados generan un valor añadido a la evolución, por un lado la

31 Mapa cromático extraído de www.gironaterritoricardioprotegit.cat, que indica la distribución territorial de desfibriladores en toda la demarcación de Girona.

administración utilizando el ingenio y la eficiencia, y por otra parte los usuarios aportando la inquietud por lo nuevo y el autoaprendizage.

Sin duda los primeros pasos de la e-administración, serán los cimientos de la e-administración venidera, generando unos roles de interacción entre administraciones y ciudadanos difíciles de imaginar hace un tiempo. Todo conlleva a pensar que el perfil de ciudadano también está cambiando, apostando por un perfil involucrado con la sociedad y con la gestión pública. Ingredientes clave entonces para el éxito de las TIC en la administración pública como instrumento de proximidad y sencillez de tramitación.

4. BIBLIOGRAFÍA

Andersen, D. F.; Dawes, S. S. (1991). Government Information Management. A Primer and Casebook. Englewood Cliffs, NJ: Prentice Hall.

Andersen, K.V.; Henriksen, H.Z. (2006), «E-government maturity models: Extension of the Layne and Lee model. Government Information Quarterly, 23 (2),. 236-248.

Australian National Auditing Office, (1999), Electronic Service Delivery, including Internet use by Commonwealth Government Agencies, ANAO. Canberra.

Barki, H.; Rivard, S.; Talbot, J. (1993). Toward an assessment of software development risk. Journal of Management Information Systems, 10, 203–223.

Berkley, B; Gupta, A(1994). Improving service quality with information tecnology. International Journal of Service Industry Management 14, 109-121.

Christou, G.; Simpson, S. (2009) New Governance, the Internet and Country Code Top Level Domains in Europe. Governance, 22 (4), 599-624.

Coursey, D.; Norris, D.F. (2008) Models of E-Government: Are They Correct? An Empirical Assessment. Public Administration Review, 68 (3), 523-536.

Criado Grande, J. I (2004). Construyendo la e-administración local, Madrid. Euro-Gestión Pública.

Criado Grande, J.I.; Ramilo, M.C. (2001). e-Administración: ¿Un reto o una nueva moda? Problemas y perspectivas de futuro en torno a internet y las tecnologías de la información y la comunicación en las administraciones públicas del siglo XXI. Recuperado el 20 de febrero de 2014, en http://www.ivap.euskadi.net/r612347/es/contenidos/informacion/rev_vasca_adm_publ/es_3822/adjuntos/ramilocriado.pdf

Díaz Méndez, A.; Cuellar Martín, E. (2007). La administración inteligente. Ministerio de Administraciones Públicas.

Fundación Telefónica (2007).Las TIC en la Administración Local del Futuro. Ariel. Madrid. Recuperado el 13 de febrero de 2014, en http://e-libros.fundacion.telefonica.com/ticenadmin/pdf/TICenlaAdminLocaldelFuturo.pdf

Gandía, J.L.; Archidona, M.C. (2008) Determinants of Web Site Information by Spanish City Councils. Online Information Review, 32 (1), 35-572500

Gil-García, J.R.; Pardo, T.A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. Government information Quarterly, 22, 187-216.

Guillamón, M.D.; Ríos, A.M.; Vicente, C. (2011) Transparencia financiera de los municipios españoles. Utilidad y factores relacionados. Auditoría Pública, 55, 109-116.

Hiller, J; Bélanger, F, (2001) Privacy strategies for electronic government, E-government series. Arlington, VA: Pricewaterhouse Coopers Endowment for the Business of Government.

Jaeger, P.T.; Matteson, M. (2009) E-Government and Technology Acceptance: The Case of the Implementation of Section 508 Guidelines for Websites. Electronic Journal of e-Government, 7 (1), 87-98.

Lara Navarra, P.; Martínez Usero, J. A. (2003). Desarrollo de sitios web para la oferta de servicios característicos de la Administración electrónica. El professional de la información, 12 (3), 190-199.

Layne, K.; Lee, J.W. (2001) Developing Fully Functional E-Government: A Four Stage Model. Government Information Quarterly, 2, 122-136.

López Tallón, A. (2010).Manual práctico de supervivencia en la administración electrónica. Creative Commons. Recuperado el 13 de febrero de 2014, en http://www.microlopez.org/downloads/docs/Manual_Supervivencia_eAdmin.pdf

Llorca Ponce, A.; Fernández Durán, L.; Pérez Montiel, M. (2008). Influencia de las TIC en la gestión urbana actual, situación en los ayuntamientos españoles. Economía industrial, 370, 153-162.

Moon, M.J.; Norris, D.F. (2005) Does Managerial Orientation Matter? The Adoption of Reinventing Government and E-Government at the Municipal Level. Information System Journal, 15 (1), 43-60.

Moon, M.J. (2002) The Evolution of E-Government among Municipalities: Rhetoric or Reality?. Public Administration Review, 62 (4), 424-433.

Pina, V.; Torres, L.; Royo, S. (2010) Is E-Government Promoting Convergence Towards More Accountable Local Governments?. International Public Management Journal, 13 (4), 350-380.

Riley, T. (2001) Electronic Governance and Electronic Democracy: Living and Working in the Connected World, Commonwealth Heads of Government Meetings, Brisbane, Australia.

Rodríguez-Domínguez, L.; Gallego-Álvarez, I.; García-Sánchez, I.M. (2009) Relación entre Factores Políticos y el Desarrollo de un Gobierno Electrónico Municipal Participativo. Análisis Local, 84, 15-26.

Siau, K.; Long, Y. (2005) «Synthesizing e-government stage models - a meta-synthesis based on meta-ethnography approach. Industrial Management + Data Systems, 105 (3/4), 443.

Statskontoret, 2000:41 (2000), The 24/7 Agency: Criteria for 24/7 Agencies in the Networked Public Administration, Statskontoret, Stockholm.

Torres, L.; Pina, V.; Acerete, B. (2006) E-Governance Developments in European Union Cities: Reshaping Government's Relationship with Citizens. Governance: An In-ternational Journal of Policy, Administration, and Institutions, 19 (2), 277-302.

United Nations Department of Economic and Social Affairs (2013). United Nations E-Government Survey 2012. UN. Recuperado el 25 de febrero 2014, en http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

Waseda University Institute of e-government (2013). Waseda University International e-Government Ranking. Recuperado el 25 de febrero 2014, en http://www.waseda.jp/eng/news11/120224_egov.html

10 AÑOS DE FIRMA ELECTRÓNICA RECONOCIDA: ¿HA TENIDO ALGÚN IMPACTO SIGNIFICATIVO EN LA E-ADMINISTRACIÓN?

Ignacio Alamillo Domingo
Investigador del GRISC, Universitat Autònoma de Barcelona

Nuria Cuenca León
Letrada de la Universitat Oberta de Catalunya

RESUMEN: La Ley 59/2003, de 19 de diciembre, define el concepto de firma electrónica reconocida, siguiendo las pautas establecidas en la Directiva 1999/93/CE, de 13 de diciembre, y en aplicación del principio de equivalencia funcional, le atribuye el mismo valor que a la firma manuscrita, así como un régimen reforzado de eficacia en caso de conflicto, creando un sistema de firma que, en el caso de los documentos privados, tiene más eficacia legal que la propia firma escrita. Sin embargo, incluso con estas indudables ventajas legales, el uso de la firma electrónica reconocida en la Administración electrónica resulta más bien escaso, e incluso cabe dudar de la existencia de una verdadera política pública de fomento de este instrumento. Como se muestra en esta comunicación, la legislación de Administración española y europea parece apostar, más bien, por otras modalidades de firma electrónica con menor valor, aunque mayor facilidad de uso, tendencia que se aprecia también en legislación sectorial, como en el caso de la contratación electrónica o del uso de la factura electrónica. La comunicación aporta una retrospectiva legal respecto a los niveles de firma electrónica exigidos a los ciudadanos, explora las posibles razones que están motivando este cambio de paradigma, en especial a la luz del Derecho europeo, y aporta algunas conclusiones sobre el futuro de la firma electrónica reconocida.

PALABRAS CLAVE: Firma electrónica, Certificado electrónico, Identificación electrónica, Administración electrónica, Autenticación electrónica.

1. INTRODUCCIÓN

La Ley 59/2003, de 19 de diciembre, define el concepto de firma electrónica reconocida, siguiendo las pautas establecidas en la Directiva 1999/93/CE, de 13 de diciembre, y en aplicación del principio de equivalencia funcional, le atribuye el mismo valor que a la firma manuscrita; e incluso, por vía del establecimiento de una presunción legal de autenticidad, en la Ley 56/2007, de 28 de diciembre, dota a la firma electrónica reconocida de un régimen reforzado de eficacia en caso de conflicto, creando un sistema de firma que, en el caso de los documentos privados, tiene más eficacia legal que la propia firma escrita.

Sin embargo, incluso con estas indudables ventajas legales, el uso de la firma electrónica reconocida en la Administración electrónica resulta más bien escaso, e incluso

cabe dudar de la existencia de una verdadera política pública de fomento de este instrumento. Como se muestra en esta comunicación, la legislación de Administración española y europea parece apostar, más bien, por otras modalidades de firma electrónica con menor valor, aunque mayor facilidad de uso, tendencia que se aprecia también en legislación sectorial, como en el caso de la contratación electrónica o del uso de la factura electrónica.

Esta política legislativa ha restringido el uso de la firma electrónica reconocida de forma extraordinaria, hasta el punto de generar dudas acerca de su viabilidad futura; y sin embargo, el futuro Reglamento europeo de servicios de confianza continúa apostando por este mecanismo, en una aparente descoordinación legislativa.

En esta comunicación realizamos una retrospectiva legal respecto a los niveles de firma electrónica exigidos a los ciudadanos, evaluando en qué medida se exige o no la firma electrónica reconocida en diversos sectores relacionados con la Administración electrónica, entendida en sentido amplio; se exploran las posibles razones que están motivando este cambio de paradigma, en especial a la luz del Derecho europeo, y se aportan algunas conclusiones sobre el futuro de la firma electrónica reconocida.

2. LA FIRMA ELECTRÓNICA EN EL ÁMBITO DEL PROCEDIMIENTO ADMINISTRATIVO

El camino de la Administración electrónica, y también el de la aplicación efectiva de la firma electrónica avanzada, se inicia en el Estado Español con la previsión, contenida en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas y del Procedimiento Administrativo Común (LRJAP-PAC), del impulso por parte de las administraciones públicas del uso de las técnicas y medios electrónicos, informáticos y telemáticos en el desarrollo de su actividad y el ejercicio de sus competencias. Dicha ley preveía que, siempre que fuera posible, los ciudadanos debían poder relacionarse con las administraciones públicas a través de medios electrónicos, sin configurar dicha posibilidad como un derecho del ciudadano, sino más bien como una concesión graciable por parte de la Administración (Gónzalez y González, 2012: pp. 920-921: Valero Torrijos, 2007: p. 3).

Ahora bien, la puerta que tímidamente abrió la LRJAP-PAC a los medios electrónicos tardó en desarrollarse, ya que no se vuelven a ver muestras de un verdadero impulso de la administración electrónica hasta la aprobación del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y de la Ley 66/1997, de 30 de desembre, de medidas fiscales, administrativas y del orden social que en su artículo 81 faculta a la Fábrica Nacional de Moneda y Timbre (FNMT) para que opere como prestadora de los servicios técnicos y administrativos necesarios para garantizar la seguridad,

validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos, en las relaciones entre las administraciones públicas entre sí, y entre éstas y las personas físicas o jurídicas.

En este contexto, y unos meses antes de la aprobación de la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica, el Estado Español aprueba el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, con la intención de dar a los ciudadanos elementos de confianza en los sistemas de comunicación electrónica a través de firma electrónica para así permitir su introducción y rápida difusión. El Real Decreto-ley pretendía dar eficacia jurídica a la firma electrónica y establecer el régimen aplicable a los prestadores de servicios de certificación, así como el régimen de infracciones y sanciones, si bien contenía una serie de diferencias relevantes con la Directiva europea aprobada sólo tres meses después (Martínez Nadal, 2001: p. 31).

El Real Decreto-ley 14/1999, igual que la Directiva 1999/93/CE, establecen las primeras definiciones legales en relación a la firma electrónica. Así, quedan establecidas, entre otras, las siguientes definiciones:

- Firma electrónica: Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.
- Firma electrónica avanzada: Es la firma electrónica que permite la identificación del firmante y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.
- Certificado: Es la certificación electrónica que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- Certificado reconocido: Es el certificado que contiene la información descrita en la ley y es expedido por un prestador de servicios de certificación que cumple los requisitos establecidos por la ley.

Además, el Real Decreto-ley y la Directiva europea, establecen que la firma electrónica avanzada siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de la firma, tiene, en cuanto a los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y es admisible como prueba en un juicio. No obstante, la ley también establece que la firma electrónica que no cumpla todos los requisitos de la firma electrónica avanzada basada en un certificado reconocido, no se le pueden negar efectos jurídicos ni puede ser excluida como prueba en un juicio, sólo por el hecho de presentarse en forma electrónica.

Después de 4 años de aplicación del Real Decreto ley 14/1999, se aprueba la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE), que deroga la normativa an-

terior, que nace con la vocación de aportar confianza a las transacciones telemáticas y comunicaciones electrónicas, desde el convencimiento que la regulación de la firma electrónica paliará la falta de confianza de la ciudadanía y así, se dará un nuevo impulso a la sociedad de la información y a la administración electrónica.

En lo que interesa en este trabajo, dos son las novedades de la nueva ley de firma electrónica:

- Se explicita la regulación de la «firma electrónica reconocida», que la LFE define como la firma avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma, a la que asigna el efecto jurídico típico de la equiparación con la firma escrita.
- Se regula el Documento Nacional de Identidad electrónico que se configura como un certificado electrónico reconocido con vocación de ser utilizado de manera generalizada en las comunicaciones electrónicas puesto que, acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos.

Así las cosas, una vez fijado el ámbito jurídico de la firma electrónica se trataba que en el desarrollo reglamentario del Estado se concretara el uso de la firma electrónica en su actividad ordinaria y de relación con los ciudadanos, de tal manera que en la medida que el Estado apostara por una determinada política de firma electrónica y fuera coherente con esta, el uso de ésta podría llegar a ser generalizado, tal y cómo se pretendía con la aprobación de la ley.

Ahora bien, como veremos seguidamente, el Estado no ha seguido una política coherente en el establecimiento de los requisitos de firma electrónica exigidos para las diferentes comunicaciones electrónicas que los ciudadanos pueden realizar con la administración, este hecho ha comportado una proliferación de certificados electrónicos que no han facilitado que el ciudadano incorpore el uso de la firma electrónica en su cotidianidad cómo sería deseable.

A partir de la aprobación de la legislación de firma electrónica (primero del RDL 14/199 y posteriormente, de la LFE), el Estado a través de disposiciones reglamentarías empieza a fijar su política de implementación de la firma electrónica en los diferentes ámbitos de su actividad.

Uno de los primeros ámbitos donde se desarrolla con intensidad el uso de la firma electrónica es el tributario, donde la importante Orden HAC/1181/2003, de 12 de mayo[1], regula el procedimiento de admisión de los sistemas de firma electrónica ade-

1 Por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.

cuados, y específicamente los sistemas de firma electrónica avanzada basada en un certificado electrónico reconocido creado mediante dispositivo seguro de creación de firma. En dicha Orden, la Administración hace una supuesta apuesta por la firma electrónica reconocida, a pesar de que admite los certificados de la FNMT-RCM, que no funcionan con dispositivos seguros, indicando en la página web de la Agencia Estatal de Administración Tributaria (AEAT) que ésta aceptará dispositivos seguros de creación de firma consistentes en aplicaciones informáticas de amplio uso, como módulos criptográficos normalizados contenidos en sistemas operativos u otro software.

En el mismo sentido se expresa la Orden ECO/2579/2003, de 15 de septiembre[2], derogada por la Orden EHA/3636/2005, de 11 de noviembre[3], que mantiene el mismo criterio, derogada por la Orden EHA/693/2008, de 10 de marzo[4], derogada por la Orden EHA/1198/2010, de 4 de mayo[5], ya alineada con el Real decreto 1671/2009, de 6 de noviembre[6]; o la Orden EHA/1274/2007, de 26 de abril[7], que deroga la Orden HAC/2567/2003, de 10 de septiembre[8].

De fecha anterior a la ley 11/2007, se refieren las dos órdenes, literalmente, a la necesidad de tener un certificado instalado en el ordenador de quien presenta la declaración, por lo que no se puede hablar de firma electrónica reconocida, precisamente por ausencia de dispositivo seguro de creación de firma electrónica.

En sentido similar, podemos citar los siguientes instrumentos:

- La Resolución de 18 de enero de 2005, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se regula el registro y gestión de apoderamientos y el registro y gestión de las sucesiones y de las representaciones legales de incapacitados, para la realización de trámites y actuaciones en materia tri-

2 Por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos.

3 Por la que se crea el registro telemático del Ministerio de Economía y Hacienda.

4 Por la que se regula el Registro Electrónico del Ministerio de Economía y Hacienda, que ya admite también claves concertadas.

5 Por la que se regula el Registro Electrónico del Ministerio de Economía y Hacienda.

6 Por el cual se desarrolla parcialmente la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

7 Por la que se aprueban los modelos 036 de Declaración censal de alta, modificación y baja en el Censo de empresarios, profesionales y retenedores y 037 Declaración censal simplificada de alta, modificación y baja en el Censo de empresarios, profesionales y retenedores.

8 Por la que se aprueba el modelo 036 de declaración censal de alta, modificación y baja en el censo de obligados tributarios y se establecen el ámbito y las condiciones generales para su presentación.

butaria por Internet, que permite conferir poderes con una firma avanzada basada en certificado reconocido en software.

- La Resolución de 26 de julio de 2006, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre asistencia a los obligados tributarios y ciudadanos en su identificación telemática ante las Entidades Colaboradoras con ocasión de la tramitación de procedimientos tributarios y, en particular, para el pago de deudas por el sistema de cargo en cuenta o mediante la utilización de tarjetas de crédito o débito, que permite hacer pagos con certificado en software.
- La Orden PRE/1551/2003, de 10 de junio[9], que apuesta claramente por el uso de la firma electrónica avanzada basada en un certificado reconocido, y no por la firma electrónica reconocida –Orden que parece anteceder el criterio que después se consolidará en la Ley 11/2007– que indica que «los dispositivos y las aplicaciones de registro y notificación sólo admitirán la firma electrónica avanzada basada en un certificado reconocido que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997) de acuerdo con lo previsto en la legislación de firma electrónica». Esta Orden fue derogada por la Orden PRE/878/2010, de 5 de abril[10], que ya aplica los criterios de la Ley 11/2007 y, por lo tanto, admite la firma electrónica avanzada basada en un certificado reconocido.
- La Orden PRE/989/2004, de 15 de abril[11], que sólo admite en el anexo III el certificado de la FNMT-RCM, en franca contradicción con la Orden PRE/1551/2003.
- El Acuerdo de 15 de septiembre de 2006, del Consejo de la Comisión Nacional del Mercado de Valores[12], que aunque se refiere expresamente a la firma reconocida en realidad admite la firma avanzada basada en un certificado reconocido. Este acuerdo fue derogado por el Acuerdo de 16 de noviembre de 2011, del Consejo de la Comisión Nacional del Mercado de Valores[13], ya alineado con la ley 11/2007 y el Real decreto 1671/2009.

---

9 Por la que se desarrolla la Disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

10 Por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre.

11 Por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos por el Ministerio de la Presidencia y los organismos públicos adscritos al departamento y se crea un registro telemático para la presentación de escritos y solicitudes.

12 En relación con la adaptación del Sistema CIFRADOC/CNMV a los servicios de certificación y firma electrónica reconocida y se crea el Registro Telemático de la Comisión Nacional del Mercado de Valores.

13 En relación con la adaptación del Sistema CIFRADOC/CNMV a los servicios de certificación y firma electrónica reconocida y se crea el Registro Telemático de la CNMV, absorbido por el registro electrónico.

- La Orden PRE/1563/2006, de 19 de mayo[14], que habla de firma digital y además impone el uso del certificado de ciudadano de la FNMT-RCM para este trámite.
- Finalmente, la Orden ITC/2308/2007, de 25 de julio, por la que se determina la forma de remisión de información al Ministerio de Industria, Turismo y Comercio sobre las actividades de suministro de productos petrolíferos que permite indistintamente la firma avanzada basada en un certificado, el DNI-e y la contraseña.

En cambio, sólo se encuentran escasos instrumentos que se refieren a la firma electrónica reconocida:

- La Orden ITC/1475/2006, de 11 de mayo[15], que se refiere a la firma electrónica reconocida del funcionario que compulsa.
- El Real Decreto 686/2005, de 10 de junio[16], que exige la firma electrónica reconocida del interventor, al menos formalmente, si bien de nuevo se admite el uso del certificado en software, y en concreto, el de la FNMT-RCM.

Como se puede ver, una simple revisión de la normativa en materia de procedimiento administrativo electrónico muestra como desde el principio ha existido una apuesta clara de la Administración en favor del uso de la firma electrónica avanzada basada en certificado electrónico reconocido, en detrimento (o como complemento, si se quiere ver así) de la firma electrónica reconocida.

Esta orientación normativa de uso amplio de la firma electrónica avanzada, en detrimento de la imposición de la firma electrónica reconocida, así como las dificultades de uso de los sistemas basados en tarjetas con microprocesador, como el DNIe, que es la principal firma electrónica reconocida de la que disponen los ciudadanos, ha motivado que, en 2012, sólo el 2,42 por ciento de las transacciones en administración electrónica se hayan sustanciado con esta firma electrónica reconocida (MHAP, 2014: p.42), a pesar de haberse distribuido al menos la cantidad de 32.464.124 DNIe a diciembre de ese mismo año (OBSAE, 2012: p.3).

En efecto, autores como Rossnagel, 2006, han observado disfunciones en la firma electrónica reconocida que afectan negativamente a la percepción de facilidad de uso o de utilidad: por una parte, la firma electrónica reconocida actúa como complemento de la firma manuscrita, y no como sustituto, debido a la necesidad de firmar desde el PC

14 Por la que se regula el procedimiento para la remisión telemática de las disposiciones y actos administrativos de los departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado».

15 Sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio.

16 Por el que se modifica el Real Decreto 2188/1995, de 28 de diciembre, por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Administración del Estado.

del usuario; por otra, la firma electrónica reconocida es una innovación preventiva respecto a las transacciones electrónicas sin firma, y requiere del acuerdo de los receptores de firmas para desplegarse adecuadamente, lo cual implica la necesidad de asumir los costes antes de tener garantía de la aceptación por los terceros. Todo ello limita la aceptación social rápida de estas tecnologías, aunque no tiene porqué limitar la adopción de tecnologías alternativas, o de las mismas tecnologías con modelos diferentes.

En este mismo sentido, de Pablo, 2012, ha puesto de manifiesto el éxito de la experiencia de la AEAT, donde la incorporación de una nueva modalidad de firma electrónica del ciudadano, consistente en un código de referencia, ha implicado un incremento de hasta el 50% en el volumen de declaraciones tributarias realizadas por Internet

3. LA FIRMA ELECTRÓNICA EN EL ÁMBITO DE LA FACTURACIÓN ELECTRÓNICA

La factura electrónica se introduce en nuestro ordenamiento jurídico a través de la Directiva 2001/115/CE del Consejo, de 20 de diciembre de 2001, por la que se modifica la Directiva 77/388/CEE con objeto de simplificar, modernizar y armonizar las condiciones impuestas a la facturación en relación con el impuesto sobre el valor añadido. El artículo 2 de dicha Directiva establecía que los Estados miembros no podían exigir que las facturas estuvieran firmadas, en referencia a las facturas en papel. No obstante, en relación a las facturas electrónicas imponía el uso de la firma electrónica reconocida, del sistema de intercambio electrónico de datos (EDI) o de otros medios, siempre que los mismo fueran aceptados por los Estados miembros.

Esta previsión en relación con la factura electrónica es la misma que, posteriormente, se estableció en la Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido, que refundió la normativa anterior.

En consecuencia con las previsiones de las Directivas, el artículo 18.1 del Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido, habilitó la posibilidad de exigir una firma electrónica reconocida para las facturas remitidas por medios electrónicos.

No obstante, el uso de la firma reconocida en este ámbito no fue muy utilizado, ya que para los usuarios era mucho más simple utilizar el certificado de la FNMT-RCM, que cabe recordar de nuevo que no se puede considerar firma reconocida (porque no dichas firmas no se crean empleando un dispositivo seguro de creación de firma electrónica), y otros certificados basados en software.

Por ello, la Agencia Estatal de Administración Tributaria optó por acudir a la alternativa prevista en el artículo 18.1.c) del Real Decreto 1496/2003, y autorizar el uso

en el ámbito de la factura electrónica los certificados admitidos para la relación jurídica tributaria, en virtud de la Orden HAC/1181/2003, y el artículo 3 de la Orden EHA/962/2007, de 10 de abril[17].

En resumen, aunque formalmente parezca que se promueve el uso de la firma electrónica reconocida, en realidad, también se abre la puerta a otros tipos de firma que acaban, en la práctica, siendo mucho más utilizadas por los usuarios, por el fácil acceso que tienen a ellas.

El ejemplo más importante lo encontramos en el artículo 4 de la Orden PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares, que claramente apuesta por la firma electrónica avanzada[18], en línea con el criterio ya establecido en la Administración electrónica.

Posteriormente, la Directiva 2010/45/UE, de 13 de julio de 2010, por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a las normas de facturación se aprueba con el objetivo de remover los obstáculos existentes en relación a la implementación de la firma electrónica para que no suponga aumentar la carga administrativa de las empresas. En este sentido, la Directiva adopta un enfoque tecnológicamente neutral[19].

---

17 Por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.

18 En concreto, dicha norma establece que «la autenticidad del origen e integridad del contenido de las facturas electrónicas que tengan por destinatario las Administraciones Públicas a las que se aplica la presente orden, en el ámbito de la contratación administrativa, así como la de aquellas que, expedidas entre particulares, se presenten telemáticamente ante tales Administraciones Públicas en el curso de cualquier procedimiento administrativo, se garantizará mediante la exigencia de firma electrónica avanzada, en los términos previstos en el artículo 3.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica».

19 La Directiva reconoce que «las facturas deben reflejar entregas o prestaciones reales y debe garantizarse por tanto su autenticidad, integridad y legibilidad. Los controles de gestión pueden utilizarse para establecer pistas de auditoría fiables entre las factures y las entregas o prestaciones, garantizando de esta forma que cada factura (ya sea en papel o en formato electrónico) cumple estos requisitos» (considerando 10), y que «La autenticidad e integridad de las facturas electrónicas puede garantizarse también mediante la utilización de determinadas tecnologías existentes, tales como el intercambio electrónico de datos (EDI) y los sistemas avanzados de firma electrónica. No obstante, puesto que existen otras tecnologías, no debe exigirse a los sujetos pasivos la utilización de una tecnología específica de facturación electrónica» (considerando 11).

Así las cosas, el artículo 233.1 de la Directiva establece que «cada sujeto pasivo determinará el modo de garantizar la autenticidad del origen[20], la integridad del contenido[21] y la legibilidad de las facturas. Podrá realizarse mediante controles de gestión que creen una pista de auditoría fiable entre la factura y la entrega de bienes o la prestación de servicios»; esto es, establece un fuerte principio de libertad de forma respecto a estas cuestiones.

Con la nueva regulación ya no se fomenta el uso de ningún tipo de firma electrónica en particular, sin perjuicio de la posibilidad de acudir a los sistemas anteriormente obligatorios, para mayor seguridad jurídica, pero en clave voluntaria.

En este sentido se expresan también los artículos 8 y 10 el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, que transpone la citada Directiva. En este sentido el artículo 8.3, sobre medios de expedición de las facturas, determina que «la autenticidad del origen y la integridad del contenido de la factura, en papel o electrónica, podrán garantizarse por cualquier medio de prueba admitido en Derecho», que «en particular, la autenticidad del origen y la integridad del contenido de la factura podrán garantizarse mediante los controles de gestión usuales de la actividad empresarial o profesional del sujeto pasivo» y, finalmente, que «los referidos controles de gestión deberán permitir crear una pista de auditoría fiable que establezca la necesaria conexión entre la factura y la entrega de bienes o prestación de servicios que la misma documenta».

Mientras que, por su parte, el artículo 10 concreta que «la autenticidad del origen y la integridad del contenido de la factura electrónica podrán garantizarse por cualquiera de los medios señalados en el artículo 8.

En particular, la autenticidad del origen y la integridad del contenido de la factura electrónica quedarán garantizadas por alguna de las siguientes formas:

a) Mediante una firma electrónica avanzada de acuerdo con lo dispuesto en el artículo 2.2 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, basada, bien en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas, de acuerdo con lo dispuesto en los apartados 6 y 10 del artículo 2 de la mencionada Directiva, o bien, en un certificado reconocido, de acuerdo con lo dispuesto en el apartado 10 del artículo 2 de la mencionada Directiva. […]».

Hay que notar, en este caso, que a diferencia de la Directiva 2010/45/UE, que se refiere a la posibilidad de uso de la firma electrónica reconocida en cumplimiento de

20 Se entenderá por «autenticidad del origen» la garantía de la identidad del proveedor de los bienes o del prestador de los servicios o del emisor de la factura.

21 Se entenderá por «integridad del contenido» que el contenido requerido con arreglo a lo dispuesto en la presente Directiva no ha sido modificado.

la norma, la regulación española ha explicitado el uso de la firma electrónica avanzada, siempre que la misma se base en certificado reconocido.

Finalmente, la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público sí apuesta por la firma electrónica, ya que de hecho su artículo 5.1 impone que «las facturas electrónicas que se remitan a las Administraciones Públicas deberán tener un formato estructurado y estar firmadas con firma electrónica avanzada basada en un certificado reconocido, de acuerdo con lo dispuesto en el artículo 10.1 a) del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación».

Como se puede ver, de nuevo se manifiesta una cierta contradicción entre la supuesta apuesta por la firma electrónica reconocida y la práctica de admitir (e incluso fomentar) el uso de la firma electrónica avanzada basada en certificado reconocido.

Contradicción que resulta palmaria, además, con la recientemente aprobada Directiva 2104/55/UE, del Parlamento Europeo y del Consejo de 16 de abril de 2014 relativa a la facturación electrónica en la contratación pública, que directamente considera que «la norma europea sobre facturación electrónica no debe contener el requisito de la firma electrónica como uno de sus elementos», por lo que cabe dudar acerca del futuro de esta cuestión en la Ley 25/2013, que no resultaría oponible a contratistas de terceros Estados miembros desde la fecha máxima de transposición de esta Directiva, que es el 27 de noviembre de 2018.

4. LA FIRMA ELECTRÓNICA EN EL ÁMBITO DE LA CONTRATACIÓN PÚBLICA

El impulso de la firma electrónica en la contratación pública se estableció inicialmente en la Directiva 2004/18/CE del Parlamento Europeo y del Consejo de 31 de marzo de 2004 sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios, que prescribe que los procedimientos de adjudicación de contratos públicos y las normas aplicables a los concursos de proyectos exigen un nivel de seguridad y confidencialidad superior al requerido en el ámbito del comercio electrónico *inter privatos*, y aconseja el fomento de las firmas electrónicas avanzadas en la contratación pública.

En concreto, el artículo 42.1.b) de la Directiva 2004/18/CE prevé que con arreglo al artículo 5 de la Directiva 1999/93/CE, los Estados miembros podrán exigir que las ofertas transmitidas por vía electrónica vayan acompañadas de una firma electrónica avanzada de conformidad con lo dispuesto en el apartado 1 de dicho artículo.

Igualmente, el anexo X.a) de la Directiva indica que las firmas electrónicas relativas a las ofertas, a las solicitudes de participación y a los envíos de planos y proyectos deben

ajustarse a las disposiciones nacionales en aplicación de la Directiva 1999/93/CE. Es decir, desde la Unión Europea se apuesta claramente por la firma electrónica avanzada, mientras que, como veremos, la legislación en materia de contratación pública española apuesta por la firma electrónica reconocida.

Así, la letra f) de la disposición adicional decimosexta relativa al uso de medios electrónicos, informáticos y telemáticos en los procedimientos de contratación del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público establece que, todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato deben ser autenticados mediante una firma electrónica reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y que, los medios electrónicos, informáticos o telemáticos empleados deben poder garantizar que la firma se ajusta a las disposiciones de la Ley de firma electrónica.

No obstante, el legislador ha querido que en el ámbito de la facturación electrónica se rebajen los requisitos en relación a la firma electrónica a utilizar, ya que en este ámbito se acepta la firma avanzada basada en un certificado reconocido. Así se refleja cuando, a través de la Ley 11/2013, de 26 de julio, de medidas de apoyo al emprendedor y de estímulo del crecimiento y de la creación de empleo, se modifica la ley en materia de contratos del sector público para establecer que las facturas electrónicas que se emitan en los procedimientos de contratación se regirán en este punto por lo dispuesto en la normativa especial de factura electrónica.

En el mismo sentido, se expresa la modificación efectuada por la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público a la letra f) de la disposición adicional decimosexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, que ya se refiere al uso de la firma electrónica avanzada.

Por último, hay que analizar lo que establece la recientemente aprobada Directiva en materia de contratación pública, de 15 de enero de 2014. La Directiva, que debe ser traspuesta por los Estados miembros en el plazo de 2 años, establece en el apartado 6 del artículo 22[22] un verdadero derecho al uso de la firma electrónica avanzada basada

22 Dicho artículo establece que «además de los requisitos establecidos en el anexo IV, se aplicarán a las herramientas y dispositivos de transmisión y recepción electrónica de las ofertas y de recepción electrónica de las solicitudes de participación las normas siguientes: [...] c) cuando los Estados miembros o los poderes adjudicadores, actuando en el marco general establecido por el Estado miembro de que se trate, concluyan que el nivel de riesgo, evaluado de conformidad con la letra b) del presente apartado, es tal que se exijan las firmas electrónicas avanzadas definidas en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, los poderes adjudicado-

en certificado reconocido, en detrimento del nivel superior de calidad y seguridad de la firma electrónica reconocida.

5. CONCLUSIONES

Como se puede ver, en todos los ámbitos analizados se observa una fuerte contradicción entre el fomento normativo de la firma electrónica reconocida y la práctica que se ha ido adoptando en la realidad.

Resulta particularmente interesante el análisis temporal de las normas de los tres ámbitos estudiados de Administración electrónica: procedimiento administrativo electrónico, facturación electrónica y contratación pública electrónica.

En un primer momento, coetáneo o cercano a la aprobación de la legislación, europea y española, de firma electrónica, las normas han exigido el uso de la firma electrónica reconocida, pero interpretando de forma amplia (o sencillamente ignorando) la exigencia del dispositivo seguro de creación de firma electrónica. Esta praxis ha permitido que la Administración acepte el uso de la firma electrónica avanzada basada en certificado reconocido por parte de los ciudadanos, pero en condiciones de inseguridad jurídica evidente, porque es el ciudadano el que debe dotarse del sistema de firma electrónico idóneo, bajo su responsabilidad, lo cual no es fácil cuando la propia Administración dota a los ciudadanos de sistemas de firma electrónica que no cumplen todos los requisitos legales.

---

res aceptarán las firmas electrónicas avanzadas respaldadas por un certificado reconocido[…], creada con o sin dispositivo seguro de creación de firma, siempre que se cumplan las siguientes condiciones:

i) los poderes adjudicadores determinarán el formato de la firma electrónica avanzada sobre la base de los formatos establecidos en la Decisión 2011/130/UE de la Comisión y establecerán las medidas necesarias para poder procesar técnicamente estos formatos; en caso de que se utilice un formato distinto de firma electrónica, la firma electrónica o el documento electrónico portador incluirá información sobre las posibilidades de validación existentes, que serán competencia del Estado miembro. Las posibilidades de validación permitirán al poder adjudicador validar en línea, gratuitamente, y sin que sea necesario conocer la lengua original, la firma electrónica recibida como firma electrónica avanzada respaldada por un certificado reconocido. Los Estados miembros notificarán información sobre el proveedor de servicios de validación a la Comisión, que se encargará de que la información recibida de los Estados miembros esté disponible para el público en Internet;

ii) cuando una oferta vaya firmada con el respaldo de un certificado reconocido incluido en una Lista de Confianza, los poderes adjudicadores no aplicaran requisitos adicionales que puedan entorpecer la utilización de este tipo de firma por los licitadores».

En un segundo momento, las normas analizadas han admitido o tolerado la posibilidad de empleo de la firma electrónica avanzada basada en certificado reconocido, como alternativa al uso de la firma electrónica reconocida. Esta situación ha supuesto una mejora en cuanto a la seguridad jurídica de los ciudadanos, pero siempre sujeta a la discrecionalidad de la Administración en cuanto a los certificados admitidos, con frecuentes discriminaciones a los operadores del mercado, como en el caso de admisión exclusiva del certificado de una entidad, en detrimento de las restantes.

En todos los casos, el impacto de la firma electrónica reconocida ha sido más bien escaso en el despliegue de la Administración electrónica, siendo inferior, a tenor de las estadísticas públicamente disponibles, al 5% del total de operaciones. Algo que sólo puede cualificarse como un fracaso estrepitoso de esta política pública.

Desde luego es cierto que es más que evidente, en cambio, la obsesión del regulador –que no del legislador, como hemos visto– de exigir firma electrónica avanzada basada en certificado reconocido, algo que ha sido objeto de crítica feroz de Boix Palop (2010: p. 320), cuando indica que «la continuada y reiterada tendencia a pedir firma digital vigente hasta la fecha demuestra, sin dudas, un grado de exigencia mucho mayor en el procedimiento electrónico que en el ordinario. […] Por extraños motivos asociados a un supuesto 'miedo al fraude' que se asocia, sin que se sepa muy bien por qué, a las actuaciones por vía electrónica, […] la fehaciencia parecía en todo casi indispensable. […] tardaremos un tiempo en desterrar totalmente la práctica de 'hiperproteger' el procedimiento administrativo de manera desproporcionada y en todo caso muy superior a la exigida en otros casos»; posición con la que sólo estamos parcialmente de acuerdo.

Y en tercer lugar, las normas más recientes, que modifican las anteriores, han elevado a la categoría de derecho subjetivo el uso de la firma electrónica avanzada basada en certificado reconocido, tanto en Derecho europeo como en Derecho español, por lo que se puede afirmar que prácticamente ha desaparecido cualquier incentivo legal a la adopción de la firma electrónica reconocida por parte de ciudadanos y empresas.

No significa esto que no tenga mayor eficacia la firma electrónica reconocida, pero sí que desde el punto de vista de la Administración electrónica, en todos sus ámbitos actuales, se ha equiparado, a la baja, con la firma electrónica avanzada basada en certificado reconocido, por lo que cabe esperar que los ciudadanos tengan tendencia a adoptar este sistema, en detrimento de la firma electrónica reconocida, al menos mientras ésta última resulte más difícil de emplear, y no conquiste nuevos espacios tecnológicos como la firma desde teléfonos inteligentes o tabletas, en que hoy no funciona.

Quizá el nuevo Reglamento europeo de identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, en fase de aprobación, suponga un nuevo impulso a la firma electrónica reconocida, al menos en las transacciones transfronterizas sujetas al derecho privado, ya que el mismo obliga a todos los Estados miembro a reconocer esta tipología de firma como equivalente, con independencia del lugar de creación de la misma, o del régimen de supervisión aplicable.

Nada apunta a que éste sea el caso en las transacciones con las entidades del sector público (como en los casos de la Administración electrónica, contratación pública electrónica o facturación electrónica), donde podemos prever que se consolide el uso de sistemas de firma electrónica avanzada basada en certificado reconocido, si bien con mayor nivel de interoperabilidad.

6. BIBLIOGRAFÍA

Boix Palop, A. (2010): «Previsiones en materia de neutralidad tecnológica y acceso a los servicios de la Administración», en Cotino Hueso, L. y Valero Torrijos, J. (Coords.): *Administración electrónica: la Ley/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*, Tirant lo Blanch, Valencia.

Cotino Hueso, L. (2010): «El derecho a relacionarse electrónicamente con las Administraciones y el estatuto del ciudadano e-administrado en la Ley 11/2007 y la normativa de desarrollo», en Gamero Casado, E. y Valero Torrijos, J. (Coords.): *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Cizur Menor: Aranzadi Thompson Reuters.

Gónzalez Pérez, J. y González Navarro, F. (2012). *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (5ª ed.)*. Cizur Menor: Civitas Thompson Reuters.

de Pablo, F. (2012). Entre el derecho del ciudadano y el ahorro de la Administración. *Boletic*, 40-47.

Martín Delgado, I. (2010): «Identificación y autenticación de los ciudadanos», en Gamero Casado, E. y Valero Torrijos, J. (Coords.): *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Cizur Menor: Aranzadi Thompson Reuters.

Martínez Nadal, A. (2001). *La Ley de firma electrónica (2ª ed.)*. Madrid: Civitas.

Ministerio de Hacienda y Administraciones Públicas (2014). *Informe presentado al Consejo de Ministros de 10 de enero de 2014 sobre de grado de avance de la implantación de la Administración electrónica en la Administración General del Estado*, disponible en http://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes/pae_InformeAvanceAdmin/pae_InfDescarga.html (última visita: 12/05/2014).

Observatorio de Administración Electrónica (2012). *Boletín de indicadores de Administración electrónica. Diciembre 2012*, disponible en http://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Boletines.html (última visita: 12/05/2014).

Rossnagel, H. (2006). On diffusion and confusion - Why electronic signatures have failed. In S. Fischer-Hübner, S. Furnell, & C. Lambrinoudakis (Eds.), *Trust and Privacy in Digital Business. 3rd International Conference on Trust and Privacy in Digital Business*, TrustBus 2006 (Vol. LNCS 4083, pp. 71-80). Springer.

Valero Torrijos, J. (2007): *El régimen jurídico de la e-Administración: El uso de medios informáticos y telemáticos en el procedimiento administrativo común (2ª ed)*. Granada: Comares.

EFECTOS DE LA IMPLANTACIÓN DE UN SISTEMA PÚBLICO DE CONTRATACIÓN POR MEDIOS ELECTRÓNICOS Y SU INCIDENCIA EN EL PANORAMA ESPAÑOL: MÁS ALLÁ DE UN CAMBIO DE FORMATO

Jordi Romeu Granados
Doctorando en Gobierno y Administración Pública UCM – IUIOG
Miembro del Grupo de Pesquisa de Controle Social do Gasto Público UNESP (Brasil)

Carmen Pineda Nebot
Consultora de Administraciones Públicas
Miembro del Grupo de Pesquisa de Controle Social do Gasto Público UNESP (Brasil)

Gregorio Juárez Rodríguez
Doctorando en Gobierno y Administración Pública UCM – IUIOG
Miembro del Grupo de Pesquisa de Controle Social do Gasto Público UNESP (Brasil)

RESUMEN: En pleno siglo xxi, el desarrollo tecnológico está representando un papel fundamental en la forma de entender el mundo y en la manera cómo se configuran las relaciones entre los actores. Las administraciones públicas, no exentas de este fenómeno, se encuentran en un punto de no retorno, de manera que, paulatinamente, van ajustando sus actuaciones a las coordenadas que, poco a poco, el nuevo paradigma dibuja. De este modo, la contratación pública, como actividad fundamental de la administración, busca encontrar su sitio dentro de una realidad emergente, altamente compleja y tecnificada. El presente trabajo analiza, desde una óptica jurídica y politológica, las consecuencias que derivan del uso de las TIC en la contratación pública. Mostrando que el fenómeno del cambio –de un entorno «analógico» a otro «digital»– no implica únicamente una alteración morfológica, sino que se trata, de modo fundamental, de una oportunidad única para el desarrollo del Gobierno abierto, el incremento de la eficiencia y eficacia de las administraciones públicas, y también la profundización en el pleno desarrollo de algunos de los principios básicos de nuestros sistemas democráticos. Asimismo, se realiza una tarea de identificación de estos efectos dentro del ámbito contractual de las administraciones públicas españolas y se presentan algunas de las experiencias más interesantes que actualmente vienen desarrollándose en la materia.

PALABRAS CLAVE: e-Contratación, Gobierno abierto, eficiencia, eficacia, transparencia.

1. INTRODUCCIÓN

La complejidad del mundo contemporáneo, en el que las tecnologías de la información y la comunicación adquieren un papel predominante, conlleva también importantes

cambios en el modo de entender el ejercicio de la acción de gobierno. Erigiéndose el ámbito de lo público como uno de los principales entornos en los que las TIC van buscando su acomodo. De hecho, conceptos tradicionalmente utilizados como «administración», «firma» o «notificación» adquieren una nueva dimensión cuando el adjetivo «electrónica» les acompaña.

Las TIC son elementos que contribuyen a reforzar las instituciones públicas, de manera tal que el e-Gobierno y la e-Democracia pueden ayudar a superar los déficits de las administraciones en materia de transparencia y rendición de cuentas (Ramió, 2013). A su vez, el uso de internet por parte de las instituciones puede servir de instrumento para atraer la confianza de los ciudadanos de forma significativa, lo que ha podido demostrarse estadísticamente (Tolbert y Mossberger, 2006).

Ante este panorama, las compras públicas –o actividad contractual pública– están incorporando, de modo paulatino, parte de las aportaciones que la revolución tecnológica comporta. Así por ejemplo, en unos pocos años hemos pasado de la publicación de los anuncios de licitación única y exclusivamente en los boletines y diarios oficiales en formato papel, a la actual situación en la que dicho soporte prácticamente ha desaparecido, habiendo sido sustituido por su equivalente digital, y al que se han unido otros medios de difusión de los procesos contractuales, como el Perfil de Contratante o las Plataformas de Contratación.

Sin embargo, la transformación que opera en la actividad contractual pública cuando el elemento tecnológico se cruza en su camino, no supone una simple «puesta a punto» a nivel formal, sino que tiene una proyección mucho mayor. El desplazamiento de lo tangible a lo virtual implica una nueva óptica desde la que observar la contratación pública. De este modo, la verdadera implementación de los sistemas públicos electrónicos de contratación no consiste en una mera inserción de datos en páginas web, sino que contiene todo un conjunto de efectos, que ofrecen una oportunidad única de establecer lugares de encuentro a los que puedan acudir poderes públicos, operadores económicos y ciudadanos, con el fin de satisfacer tanto sus expectativas individuales como aquellas que les son comunes.

2. EL FENÓMENO DE LA CONTRATACIÓN PÚBLICA ELECTRÓNICA

La Comisión Europea entiende la e-Contratación como la introducción de medios electrónicos en el tratamiento de las operaciones y en la comunicación por parte de las instituciones gubernamentales y demás organismos del sector público a la hora de adquirir bienes y servicios o licitar obras públicas. Ello implica la sucesiva incorporación de procedimientos electrónicos que sustentarán las diversas fases del proceso de contratación: desde la propuesta de inicio del expediente hasta la facturación y pago[1]. Fases que se desarrollan en un doble ámbito: hacia dentro y hacia fuera de la organización.

1 Libro Verde sobre la generalización del recurso a la contratación pública electrónica en la Unión Europea SEC (2010) 1214.

Figura 1. Fases del proceso de contratación pública

Fuente: VORTAL Connecting Business
(*Contratación electrónica en el Sector Público Español. Eficiencia, ahorro, transparencia*)

Así pues, la e-Contratación pone de manifiesto un interés holístico en abarcar la práctica totalidad de los momentos por los que transita el proceso contractual[2], lo que de por si denota que nos hallamos ante un fenómeno no puramente testimonial o anecdótico, sino con unas repercusiones importantes.

En el proceso de impulso de la contratación pública electrónica no podemos olvidar el papel activo y protagonista que la Unión Europea ha venido asumiendo. Las Directivas 2004/18/CE y 2004/17/CE aunque supusieron un paso importante para la contratación electrónica no tuvieron los resultados esperados, pues la implementación de la misma no se estableció con carácter obligatorio[3]. Ante esta situación, la Comisión publicó en 2010 el Libro Verde sobre la generalización del recurso a la contratación pública electrónica en la Unión Europea, SEC (2010) 1214, como un primer paso hacia una revisión del marco de contratación pública de la UE.

Tras un proceso de tramitación de más de dos años, se aprueba la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE. Esta nueva norma reconoce que los medios de información y comunicación electrónicos sirven para simplificar la publicación de los contratos, aumentando la eficiencia y la transparencia de los procedimientos de contratación, razón por la cual «deben convertirse en el método estándar de comunicación e intercambio de información en los procedimientos de contratación» (Considerando 52). A su vez, se adopta una comunicación totalmente electrónica, en particular por lo que respecta a la presentación de ofertas o solicitudes de participación,

2 Aunque podría defenderse también que dicho proceso forma parte de un fenómeno mucho más amplio que arranca con la detección de la necesidad a cubrir con la actividad contractual y su correspondiente previsión económica mediante reflejo presupuestario, y finalizaría con la evaluación de los resultados obtenidos.

3 Cuya transposición en España se produjo con la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

en todos los procedimientos de licitación, con un período de transición de 30 meses. Sin embargo, la propia directiva contiene una limitación, al indicar que la misma «no debe obligar a los poderes adjudicadores a tratar electrónicamente las ofertas, como tampoco debe exigir la evaluación electrónica ni el tratamiento automatizado», y que «ningún elemento del procedimiento de contratación pública tras la adjudicación del contrato debe estar sujeto a la obligación de utilizar medios electrónicos de comunicación, como tampoco debe estarlo la comunicación interna en el marco del poder adjudicador».

3. LA E-CONTRATACIÓN Y SUS EFECTOS

A la hora de abordar los efectos derivados de la contratación pública electrónica, resulta necesario establecer una categorización de los mismos. En un esfuerzo por llevar a cabo dicha tarea podríamos identificar tres grandes grupos de efectos, en todo caso positivos, como son los técnico-administrativos, los político-sociales y los económicos.

Tabla 1. Beneficios de la e-Contratación

TÉCNICO-ADMINISTRATIVOS	• Publicidad y transparencia (proactiva) • Accesibilidad e interoperabilidad • Abierto todos los días y a todas horas (24x7x365) • Objetividad / Límite a la arbitrariedad / Igualdad de condiciones • Eficacia y eficiencia • Seguridad y trazabilidad de la información • Reducción de plazos • Innovación (*beta permanente*) • Mejora del clima laboral • Nuevos conceptos y nueva cultura (e-Contratación, e-Licitación, etc.) • Contribución a la *accountability* horizontal y a un mejor seguimiento y análisis de la actividad contractual • Simplificación y homogeneización de procedimientos
POLÍTICO-SOCIALES	• Transparencia (reactiva) • Promoción y desarrollo del Gobierno abierto • Gobernanza: interacción entre actores (gobierno en red) • Límite a la corrupción • Consolidación de las instituciones democráticas • Autocontrol de los poderes públicos • Ayuda para la implantación de otras políticas (políticas sociales, medioambientales, etc.) • Contribución a la *accountability* vertical social (control social) • Participación ciudadana • Fomento de la sociedad de la información y del conocimiento • Inteligencia colectiva

ECONÓMICOS	• Eficiencia • Concurrencia / competitividad / mejores ofertas • Ahorro de recursos, lo que permite atender a otros fines (mejora de la sociedad / fomento de la riqueza) • Proyección transfronteriza de las empresas • Dinamización de la actividad económica administrativa • Dinamización de la actividad económica general • Ayuda a las PYMES • Cohesión del mercado europeo

Fuente: elaboración propia

En relación con estos tres grandes grupos de efectos, cabe apuntar que no se trataría de compartimentos estancos, sino que las fronteras entre unos y otros se muestran difusas, por cuanto que la proyección de algunos de los beneficios enunciados es tan amplia que impide su adscripción a una única de las categorías indicadas.

En base a la clasificación establecida procedemos a analizar los efectos que consideramos más significativos.

3.1. Efectos técnico-administrativos

3.1.1. Publicidad y transparencia

En las organizaciones públicas hoy en día prevalece un tema central, que es el de la transparencia de las relaciones y la utilización de los recursos para atender a la sociedad (Rodrigues de Faria *et al.*, 2010). Y es la contratación pública una de las áreas donde mayor importancia cobra dicha institución ya que, dadas las diferentes implicaciones que aquella lleva consigo (manejo de fondos públicos, peso de la contratación pública en la actividad económica general, posible desviación a formas de corrupción, etc.), se requiere, en todo momento, eliminar cualquier atisbo de opacidad.

En este orden de cosas, la e-Contratación se manifiesta como un instrumento que facilita la transparencia (Joongi, 2006; González Alonso, 2009; Vaidya, 2009:3; Gardenal, 2010; Moreno Molina, 2011; Elezi y Harizaj, 2012; Neupane *et al.* 2012a, 2012b; Alaweti *et al.*, 2013; Pintos, 2014; Romeu *et al.*, 2014), en tanto que promueve la apertura de datos (Álvarez *et al.*, 2011) y la divulgación de los mismos. De hecho, para el Libro Verde sobre la generalización del recurso a la contratación pública electrónica en la Unión Europea SEC (2010) 1214, con ella se logra una mayor transparencia, puesto que el proceso de contratación es más abierto, está automatizado y es objeto de una mayor divulgación. A su vez, se trata de un procedimiento mejor documentado y auditado (ANEI, 2012). Así pues, el permitir un alto grado de conocimiento en tiempo real, al permanecer la administración «abierta al público» las 24 horas del día, los procesos pueden ser trazados de forma completa (preparación, inicio, publicación, licitación, adjudicación, ejecución y extinción) (Álvarez Yagüe, 2010).

Una muestra de este espíritu aperturista se ofreció ya con la incorporación a nuestro ordenamiento jurídico del Perfil de Contratante y la Plataforma de Contratación del Estado (actual Plataforma de Contratación del Sector Público) por la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. De igual manera, el Portal de Transparencia que promueve la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, supone otro avance en este sentido –aunque modesto– por cuanto que incluye la obligación de publicar en el mismo diversos aspectos relativos a la contratación pública (art. 8).

La Directiva 2014/24/UE se refiere expresamente a la genérica obligación de los poderes adjudicadores de ofrecer por medios electrónicos un «acceso libre, directo, completo y gratuito» a los pliegos contractuales (art. 53.1), lo que redunda en una evidente promoción de la transparencia contractual.

3.1.2. Accesibilidad e interoperabilidad

La accesibilidad supone proporcionar información estructurada sobre los documentos y recursos de información con vistas a facilitar la identificación y búsqueda de la información[4].

Según el Libro Verde (2010), la contratación electrónica puede mejorar el acceso de las empresas a la contratación pública gracias a la automatización y centralización del flujo de información sobre las oportunidades de licitación concretas. Así, la búsqueda en línea supone identificar oportunidades de forma rápida y a un coste reducido. Incluso los sistemas de contratación electrónica permiten la configuración, a fin de alertar a los proveedores, sobre ofertas específicas, facilitando, de ese modo, el acceso inmediato a la documentación sobre las licitaciones.

Por otra parte, la accesibilidad en materia de contratación pública es una exigencia que viene recogida por la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado (art. 8, en relación al art. 9.2.c). Sin embargo, el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público (TRLCSP) ya incluía, en su disposición adicional decimosexta, algunas previsiones relativas a favorecer dicha accesibilidad. Entre ellas, que los medios electrónicos, informáticos y telemáticos utilizables deberían ser no discriminatorios, estar a disposición del público y ser compatibles con las tecnologías de la información y de la comunicación de uso general.

El esfuerzo del legislador por hacer accesible la tecnología en los procedimientos de contratación coadyuva, a su vez, a reforzar la transparencia –a la que nos referíamos

4 Art. 11 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

anteriormente– por cuanto que se establecen los medios para que las partes no solo «hablen el mismo idioma», sino que este sea fácilmente entendible. De hecho, la Directiva 2014/24/UE aclara que la obligación de utilizar medios electrónicos en todas las fases del procedimiento de contratación no estaría justificada cuando la utilización de dichos medios requiriera de instrumentos especializados o formatos de ficheros que no estuvieran disponibles de forma general o cuando la comunicación en cuestión solo pudiera manejarse utilizando equipos ofimáticos especializados (Considerando 53).

Al mismo tiempo, directamente relacionada con la accesibilidad aparece la idea de la interoperabilidad, que es la capacidad de los sistemas de información y de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos[5].

El Libro Verde (2010) manifestaba que es conveniente fomentar soluciones que mejoren e intensifiquen la interoperabilidad de los sistemas de contratación pública locales, regionales y nacionales, lo que permitiría abolir barreras técnicas innecesarias a la participación transfronteriza en los sistemas de contratación pública electrónica. A su vez, la nueva directiva de contratación pública indica (Considerando 55) que la existencia de diferentes formatos o procesos técnicos y normas de mensajería puede suponer un obstáculo para la interoperabilidad, no solo en cada Estado miembro, sino también, de modo especial, entre los distintos Estados miembros, por lo que se requiere un esfuerzo de normalización de dichos instrumentos. Con ello se obtendrá también una mejora de la eficacia, reduciendo el esfuerzo exigido a los operadores económicos.

3.1.3. Objetividad y limitaciones a la arbitrariedad

No cabe duda que la e-Contratación supone un refuerzo al principio de objetividad que necesariamente ha de regir la actividad de las administraciones públicas[6]. Principio este de carácter transversal, al tener que aplicarse en todas las fases de un contrato público.

De hecho, si tomamos como referencia la subasta electrónica (que, junto a los sistemas dinámicos de adquisición, conforman los dos únicos procedimientos de adjudicación exclusivamente electrónicos recogidos actualmente por el legislador español) esta viene articulada a partir de un proceso iterativo basado en un dispositivo electrónico que permita la clasificación de las ofertas a través de métodos de evaluación automáticos (art. 148 TRLCSP). Y dicha automaticidad ofrece menor posibilidad a la intervención humana, lo que limita la posible influencia de políticos o funcionarios, en interés propio, a la hora de realizar adjudicaciones de contratos.

---

5 Preámbulo del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

6 Art. 103 de la Constitución Española de 1978 y art. 3.1 de la Ley 30/1992.

En este sentido, la adopción de sistemas de e-Contratación resulta necesaria para luchar contra el fraude, la corrupción, el amaño de licitaciones y las prácticas colusivas por parte de los participantes en la licitación (Panda *et al.*, 2010). A su vez, el carácter objetivo y neutral asociado a la e-Contratación es susceptible de generar un clima de confianza en los contratistas, lo que posibilitará un efecto evidente como es el del aumento de la concurrencia (Gimeno Feliu, 2011).

3.1.4. Eficacia y eficiencia

Ya en el año 2003, la Comisión Europea señalaba que las operaciones tradicionales de contratación pública son largas y dilatadas, y consumen muchos recursos, por lo que la utilización de las TIC puede resultar especialmente ventajosa, mejorando la eficacia, la calidad y la relación coste/eficacia de estos contratos[7]. Posteriormente, en el Libro Verde (2010) se señaló que la contratación electrónica, frente a los sistemas basados en el soporte papel, puede aportar considerables mejoras en materia de eficiencia de las adquisiciones concretas, gestión global de la contratación pública, funcionamiento de los mercados en el ámbito de los contratos estatales y reducción de costes derivados de la distancia geográfica, además de mejorar el seguimiento y la eficiencia global de la contratación pública y de agilizar los procedimientos de contratación.

Según González Alonso (2009:143) las bondades del procedimiento electrónico de contratación pública son evidentes: entre ellas, reducción de plazos[8], celeridad en la tramitación, incremento de la interacción entre las administraciones públicas y las empresas, mejora de los procedimientos de seguimiento y análisis de los contratos, mayor confianza en la imparcialidad de los procedimientos de adjudicación y desmaterialización de los mismos.

También para Gimeno Feliu (2011) la cultura de la contratación pública electrónica aporta ventajas desde la perspectiva de la agilización de los procedimientos de adjudicación, ayudando en el cumplimiento de los plazos establecidos, y suponiendo una minimización de errores en la mecanización de las ofertas recibidas, pues se hace vuelco de las mismas de forma automatizada. De igual modo, podemos afirmar que el propio proceso de e-Contratación, dados los flujos de información relevante y sistematizada que *per se* aporta a los gestores de la organización, posibilita una evaluación racional del gasto público, sirviendo de herramienta de gran valor para el futuro diseño de las políticas de compras públicas.

---

7 Comunicación de la Comisión, de 26 septiembre 2003, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones – El papel de la administración electrónica en el futuro de Europa COM (2003) 567. http://europa.eu/legislation_summaries/information_society/strategies/l24226b_es.htm_[25/02/14]

8 Se considera que en España se pueden reducir los plazos un 25% en las fases de presentación de proposiciones, recepción de solicitudes, recepción de ofertas y, especialmente, en los contratos sujetos a regulación armonizada (González Alonso, 2009).

Sin embargo, tal y como indica Domínguez-Macaya (2011:470), no solo es necesario que las administraciones públicas se doten de plataformas tecnológicas adecuadas, sino que es imprescindible la planificación y el desarrollo de métodos y procedimientos de despliegue de los resortes tecnológicos, organizativos y de las destrezas para hacer frente a la prestación de servicios digitales. Se trata, en última instancia, de llevar a cabo una adecuada gestión del cambio en el seno de la organización, que permita la maximización de resultados. Tarea para la cual deberán tomarse en cuenta aspectos de diversa índole, entre los que destacan: la tecnología, los procesos, las personas y el ambiente (Gardenal, 2010).

3.1.5. Seguridad y trazabilidad de la información

Que la información sea transmitida y almacenada de modo seguro es un factor crítico de éxito de la e-Contratación. Para ello, de conformidad con la disposición adicional decimosexta del TRLCSP, se deberán tomar en cuenta, entre otros, los siguientes aspectos[9]:

- Los sistemas de comunicaciones y para el intercambio y almacenamiento de información deberán poder garantizar la integridad de los datos transmitidos y que solo los órganos competentes, en la fecha señalada para ello, puedan tener acceso a los mismos.
- Las aplicaciones que se utilicen para efectuar las comunicaciones, notificaciones y envíos documentales entre el licitador o contratista y el órgano de contratación deben poder acreditar la fecha y hora de su emisión o recepción[10], la integridad de su contenido y el remitente y destinatario de las mismas.
- Todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan a lo largo del procedimiento de contratación deben ser autenticados mediante una firma electrónica avanzada reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica[11].

---

9 En cualquier caso, se estará también a lo dispuesto por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

10 El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica se refiere al «sello de tiempo» como la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

11 Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (art 3.3 Ley 59/2003, de 19 de diciembre, de firma electrónica).

Asimismo, directamente vinculada con la seguridad, otra de las características que cabe apuntar es la trazabilidad, por cuanto que el sistema electrónico a utilizar deberá disponer de mecanismos para registrar todos los sucesos y todas las actividades de los usuarios, así como los intentos de acceder a la información sensible (Domínguez-Macaya, 2011:177).

3.2. Efectos político-sociales

3.2.1. Gobierno abierto

Si, como veíamos anteriormente, el fenómeno de la e-Contratación facilita la implementación de las políticas de transparencia, de igual manera incide sobre el resto de los elementos conformadores del denominado «Gobierno abierto», como son la participación y la colaboración[12].

El pleno desarrollo de políticas de contratación pública por medios electrónicos permitiría la mayor interacción entre los actores. De un lado, posibilitaría una mayor confianza de los operadores económicos respecto de los poderes públicos adjudicadores (Kartiwi, 2006; Neupane *et al.*, 2012a), dado el carácter de objetividad y transparencia aplicado a todo el proceso. Por otra parte, supondría también un incremento en los niveles de implicación de la ciudadanía como receptora de los servicios susceptibles de contratación por la administración, pues las TIC facilitan la intervención de los particulares en el diseño de las políticas públicas, así como en el seguimiento de las mismas[13].

3.2.2. Límite a la corrupción

El Parlamento Europeo ha llegado a afirmar que el sector de la contratación pública es el más expuesto a los riesgos de gestión irregular, fraude y corrupción, y que estas conductas ilícitas distorsionan el mercado, provocan un aumento de los precios y de las tarifas abonadas por los consumidores para la adquisición de bienes y servicios, al tiempo que siembran la desconfianza con respecto a la Unión Europea. Es por ello que insta a los Estados miembros a que establezcan como máxima prioridad la lucha contra la corrupción en la contratación a través de una adecuada aplicación de las directivas sobre contratos públicos, merced a «los efectos devastadores de la corrupción en términos

12 Recogemos el ideal de *Open Government* incluido en el *Memorandum for the Heads of Executive Departments and Agencies* (White House, 2009).

13 A tal efecto, resulta revelador el documento elaborado por la Fundación Telefónica *Las TIC en el Gobierno Abierto: Transparencia, participación y colaboración.* http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/detalle/211_[03/03/14]

de inflación de costes, adquisición de equipos innecesarios, inadecuados o de calidad inferior»[14].

Para Neupane *et al.* (2012b), siendo que un principio básico de los gobiernos debería ser el adquirir el bien adecuado en el plazo adecuado y con el precio también adecuado, el proceso requiere ser abierto, objetivo y transparente. Así, algunos de los factores –los más importantes– para luchar contra la corrupción desde la e-Contratación serán: el acceso en tiempo real a la información contractual, la reducción de la intervención humana en la licitación pública, la automatización del sistema, y el refuerzo de la transparencia y la *accountability*.

3.2.3. Control social

El art. 9.2 de la Constitución Española de 1978 indica que corresponde a los poderes públicos el facilitar la participación de todos los ciudadanos en la vida política, económica, social y cultural. Y una de la manifestaciones de dicha participación vendría determinada por la posibilidad de ejercitar funciones de monitoreo y evaluación de la actividad contractual pública[15].

Al respecto, cabe indicar que las TIC se manifiestan como elementos idóneos para el fomento y desarrollo de esta facultad de control y seguimiento de la actividad de gestión de gasto público que supone la contratación administrativa. Por lo que podemos entender que la contratación pública electrónica debería postularse no solo como un medio para la mejora de las relaciones entre los poderes públicos y los operadores económicos –esto es, contratante y contratista–, sino integrando también la acción vigilante de la ciudadanía. De hecho, siguiendo a Marques *et al.* (2014), la mayor publicidad que aporta la e-Contratación proporciona, a su vez, un mayor control de la sociedad en la gestión de los recursos públicos.

3.2.4. Fomento de la sociedad de la información y del conocimiento e inteligencia colectiva

El uso regular de las nuevas tecnologías de la información y de la comunicación en la contratación pública aumenta el nivel de conocimiento de estas por parte de todos los

14 Apartado 27 de la Resolución del Parlamento Europeo, de 6 de mayo de 2010, sobre la protección de los intereses financieros de las Comunidades y la lucha contra el fraude (DOUE C81E, de 15 de marzo de 2011) y apartado 58 de la Resolución del Parlamento Europeo, de 14 de diciembre de 2011, sobre el impacto de la crisis financiera en el sector de la defensa de los Estados miembros de la UE (DOUE C168, de 14 de junio de 2013).

15 Para Di Virgilio y Solano (2012) el monitoreo es un proceso continuo y permanente, mientras que la evaluación se realiza en períodos establecidos, siendo de corte transversal.

actores participantes en el proceso. En el caso de las empresas, con independencia del tamaño de las mismas, pueden sentirse incentivadas a adoptar las TIC y las prácticas del comercio electrónico de cara a resultar adjudicatarias de posibles contratos públicos, y a desarrollar, con ello, nuevas oportunidades de negocio.

Por otra parte, existen evidencias de que las decisiones tomadas de forma conjunta por un grupo de personas suelen ser más adecuadas que las que se toman de forma individual (Surowiecki, 2004). De este modo, un mejor aprovechamiento de las oportunidades de agregación nos ayudaría a comportarnos de un modo más inteligente, ofreciéndonos una mayor calidad de vida (Figueiras, 2012). En relación con ello, las TIC pueden servir de elemento catalizador para la formación de dicha inteligencia colectiva, por lo que la aplicación de las mismas al ámbito de la contratación pública es susceptible de generar valor añadido a las relaciones entre los actores: el saber compartido que, a su vez, es susceptible de retroalimentación.

3.3. Efectos económicos

3.3.1. Mejora de la concurrencia y de la competitividad

El acceso a la contratación pública en condiciones de igualdad para todos los posibles contratistas ha sido una preocupación constante en la regulación del régimen jurídico de los contratos celebrados por los entes públicos. En este sentido, el artículo 1 del TRLCSP señala como principios fundamentales de la contratación pública «los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los candidatos».

Dicho acceso se mejora con la e-Contratación, como resaltaron tanto la Directiva 2004/17/CE como la 2004/18/CE, al indicar que las nuevas técnicas electrónicas de compra amplían la competencia y mejoran la eficacia, ahorran tiempo y dinero y, por lo tanto, suponen la utilización óptima de los fondos públicos. Asimismo, el Libro Verde (2010) hablaba del fomento de una mayor participación, mediante el incremento del número de posibles proveedores y la eventual ampliación de los mercados. Finalmente, la Directiva 2014/24/UE, si bien indica que los medios de comunicación electrónicos son especialmente idóneos para apoyar prácticas y herramientas de compra centralizadas (Considerando 72), tal centralización debe supervisarse cuidadosamente para evitar una excesiva concentración de poder adquisitivo y la colusión (Considerando 59).

El aumento en el número de proveedores, además de mejorar la relación calidad-precio, puede beneficiar a las empresas, sobre todo a las PYMES. La e-Contratación debe entenderse como una excelente oportunidad en un momento de dificultades como el actual, ya que facilita la convocatoria de concursos públicos más transparentes, posibilitando la presentación de propuestas a procesos de contratación a los que, de otro

modo, resultaría muy difícil o incluso imposible concurrir (ANEI, 2012). A su vez, la incorporación de las PYMES a la contratación transfronteriza supondría una mayor profesionalización de las mismas que, a la larga, podría incluso contribuir a una mayor creación de empleo (Vidorreta, 2013).

3.3.2. Ahorros económicos

Otra de las ventajas asociadas a la e-Contratación es el ahorro de costes. Ahorro que se produce en una doble dirección: para los operadores económicos y para las administraciones públicas.

Las empresas que participan en los procedimientos contractuales que se llevan a cabo por medios electrónicos, dejan de invertir tiempo y dinero en desplazamientos hasta la sede donde radica el órgano de contratación a fin de obtener la documentación, formular consultas o presentar sus ofertas. Por otra parte, el ahorro en papel supone también un beneficio considerable, sobre todo en aquellos supuestos en los que la propia licitación exige la presentación de proyectos o una extensa documentación complementaria (en ocasiones, con varias copias de la misma).

En relación con el ahorro para los entes públicos, este alcanza una dimensión mucho mayor. Según la Comisión Europea (2012)[16], los organismos y autoridades que ya han realizado la transición hacia la e-Contratación constatan, por lo general, ahorros de entre un 5 y un 20 por ciento, siendo los costes de inversión fácilmente recuperados.

4. LA E-CONTRATACIÓN EN ESPAÑA

Las cifras sobre el uso de la contratación electrónica en España ofrecen un panorama ciertamente limitado. En este sentido, si nos atenemos a datos correspondientes a 2013 (Eurostat), el número de empresas que habrían usado internet para acceder a la documentación y las especificaciones técnicas de las licitaciones en sistemas públicos de contratación se sitúa en un 18%, frente a la media de la UE, que es del 23%. Siendo el porcentaje de empresas españolas que han ofrecido bienes y servicios mediante sistemas electrónicos de contratación del 5%, lo que contrasta, asimismo, con la media de países de la UE, que se encuentra en el 13%.

No obstante, pese a dichos datos, poco a poco van desarrollándose iniciativas que, aunque aisladas, suponen un cierto cambio en el panorama nacional. Pasemos, pues, a mostrar algunos ejemplos.

16 Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones, COM (2012) 179 final, *A strategy for e-procurement.* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0179:FIN:EN:PDF_[01/03/14]

4.1. El Modelo de Contratación Pública Electrónica del Gobierno Vasco[17]

Se trata de una experiencia pionera en nuestro país, pues el proyecto arranca del año 2002, permitiendo en el año 2005 la primera licitación en el Estado totalmente electrónica. A su vez, ha sido objeto de numerosos reconocimientos y galardones, resultando finalista a los premios *e-Government 2009* de la Comisión Europea.

El Gobierno Vasco propone un sistema propio de contratación pública electrónica que, buscando alcanzar unos objetivos generales, mejore la competitividad y eficiencia de las empresas vascas y de la propia administración.

Entre 2005 y 2009 fueron tramitados electrónicamente 203 expedientes, cuyo presupuesto de licitación alcanzó 124,6 millones de euros. Lo que, si nos atenemos a las estimaciones de la Comisión Europea que veíamos anteriormente (disminución de gastos entre un 5% y un 20%), habría supuesto unos ahorros de entre 6 y 25 millones de euros.

Los elementos fundamentales que componen el sistema de contratación pública electrónica son la consulta de Registro de Contratistas, la información sobre concursos y licitaciones, y la licitación electrónica, que permite presentar ofertas a través de internet.

Por otra parte, se deriva una voluntad de fomentar el compromiso y participación de los actores. Así, el Gobierno Vasco pone a disposición de los usuarios multitud de canales que ofrecen información general y especializada del sistema (Servicio de Atención al Usuario *Zuzenean*, Registro Oficial de Contratos, *Izenpe*, etc.). También se ofrecen diversos cursos de formación presenciales y *on line*, manuales de usuario accesibles desde las páginas web, así como un curso completo de formación presencial ofertado completamente a través del canal *Youtube* y el acceso a licitaciones de prueba libre a disposición de los operadores económicos. Finalmente, cabe señalar que la apertura de ofertas puede seguirse «en abierto» a través de *Irekia*, el canal público vasco de internet.

4.2. El Sistema de Contratación Electrónica de la Universidad de Almería

La Universidad de Almería utiliza la Plataforma de Contratación Electrónica de la empresa Vortal, informando a los usuarios, con carácter general y en atención a las características de las diferentes dudas que surjan, a través de la página web www.vortalgov.es.

La plataforma está sirviendo de medio para la integración de las PYMES, por cuanto que la mayor parte de los licitadores y también de los adjudicatarios pertenece al grupo de pequeñas empresas y microempresas (González y Rodríguez, 2013).

17 Acceso disponible en:
https://www.euskadi.net/w32-home/es/
http://www.contratacion.euskadi.net/w32-home/eu/
[04/03/14]

4.3. El Sistema de Contratación Pública Electrónica del Ayuntamiento de Gijón

El Ayuntamiento de Gijón también ha optado por los servicios de la plataforma de contratación electrónica Vortal.

La Plataforma de Contratación Electrónica del Ayuntamiento de Gijón ha sido galardonada con el «Premio al mejor servicio operativo en Administración Electrónica en la Nube» en el IV Congreso Nacional de Interoperabilidad y Seguridad celebrado en Madrid los días 19 y 20 de febrero de 2104.

Esta plataforma se apoya en el *cloud computing* y, como novedad, permite la licitación electrónica de los contratos menores[18]. Desde el día 11 de noviembre de 2013 el Ayuntamiento de Gijón empezó a tramitar todos sus contratos menores, y los de sus empresas públicas, a través de su plataforma electrónica de licitación, lo que supone un salto considerable en términos de publicidad y transparencia, así como en la promoción de la concurrencia entre las empresas. Y todo ello sin perjuicio de los ahorros susceptibles de alcanzarse, teniendo en cuenta el tan extendido uso en la actualidad del procedimiento de la contratación menor.

5. CONCLUSIONES

Los efectos que aporta la contratación pública electrónica son múltiples, y estamos en condiciones de afirmar que, a la vista de lo anteriormente indicado, todos ellos positivos. Sin embargo, no se puede decir que la implantación de la e-Contratación en España haya tenido un éxito rotundo. Más bien al contrario, las iniciativas desarrolladas al respecto se han llevado a cabo «a pesar» de las previsiones normativas europeas y nacionales –vista la laxitud con que se ha abordado la materia desde ambos ámbitos– pues no ha habido una apuesta decidida por establecer un sistema obligatorio de contratación pública por medios enteramente electrónicos, que permita identificar el recurso a la misma como un fenómeno habitual en el ámbito de la administración.

Así, no es hasta la llegada de la nueva Directiva 2014/24/UE, que se establece la obligatoriedad del uso de la contratación pública electrónica. Pero incluyendo unos tiempos de adaptación de las normativas estatales (entre ellos, un período transitorio de 30 meses, para la presentación de las ofertas o solicitudes de participación, en cualquier procedimiento) que difícilmente encajan en una realidad administrativa y social que precisa de otro tipo de contratación pública, mucho más objetiva, dinámica y eficiente. A su vez, dejando fuera de dicha obligatoriedad a partes importantes del proceso contractual, como sucede con la evaluación de las ofertas y la ejecución del propio contrato, y obviando el importante papel de los ciudadanos, destinatarios últimos del proceso.

18 Regulados por los arts. 111 y 138.3 TRLCSP.

Por lo tanto, a fin de llegar a una contratación electrónica integral –lo que Domínguez-Macaya (2011:577) denomina la «ieContratación»–, que dé acceso pleno a los beneficios señalados en el presente trabajo, es necesario confiar en un conjunto de factores, entre los que destacan: la voluntad firme del legislador español en ir incluso más allá de las previsiones realizadas desde el ámbito comunitario (tomando ejemplo de otros países como Portugal, donde desde 2009 la contratación pública electrónica es obligatoria) y un liderazgo sólido, con visión de conjunto sobre la materia, que aborde la e-Contratación como parte indisoluble del Gobierno abierto. Propiciando, ambos elementos, un cambio de cultura que entienda la gestión de lo público desde la integración de los diferentes actores, esto es, poderes públicos, operadores económicos y ciudadanía.

6. BIBLIOGRAFÍA

Alaweti, M.F., Nurdiana, A., Faryadi, Q. (2013). The transparency of public bidding and contracting using e-Procurement in Malaysia SMPPS. International Conference on Social Science Research, Penang, Malasia, 4-5 junio 2013. http://worldconferences.net/proceedings/icssr2013/toc/404%20-%20Mohamed%20-%20The%20Transparency%20of%20Public%20Bidding%20and%20Contracting%20using%20E-Procurement%20in%20Malaysia%20SMPPs_done.pdf [25/02/14]

Álvarez Yagüe, S. (2010). Más y mejor con menos: beneficios de la contratación pública electrónica. *Dintel*, marzo, 150-151.

Álvarez, J.M., Labra, J.E., Cifuentes, F., Alor-Hernández, G., Sánchez, C., Guzman J.A. (2011). Towards a pan-European e-Procurement platform to aggregate, publish and search public procurement notices powered by linked open data: the moldeas approach. *International Journal of Software Engineering and Knowledge Engineering*. http://moldeas.googlecode.com/hg-history/da513adc4e70b8e11e-bb785465a91be65bc9c487/trunk/papers/ijseke/e-proc-ijseke.pdf [25/02/14]

Asociación Nacional de Empresas de Internet (ANEI) (2012). La Contratación Electrónica Pública en España: una necesidad inaplazable. http://www.a-nei.org/documentacion/Informe%20ANEI_Contratacion%20Electronica.pdf [08/03/14]

Di Virgilio, M., Solano, R. (2012). Monitoreo y evaluación de políticas, programas y proyectos sociales. UNICEF/Fundación CIPPEC. Buenos Aires. http://www.unicef.org/argentina/spanish/cippec_uni_monitoreo_evaluacion.pdf [09/01/14]

Domínguez-Macaya, J. (2007). La contratación electrónica en el proyecto de ley de contratos del sector público. Análisis y propuestas de mejora. *Diario LA LEY* (6656), 1-6.

Domínguez-Macaya, J. (2011). *Claves para una contratación pública electrónica eficaz*, El Consultor de los Ayuntamientos. Madrid: *La Ley*.

Elezi, E., Harizaj, M. (2012). Efficiency evaluation of the public e-Procurement system in the reduction of curruption: the Albanian case. Transatlantic Conference on Transparency Research, Utrecht, 7-9 junio 2012. http://www.transparencyconference.nl/wp-content/uploads/2012/05/Elezi-Harizaj.pdf [25/02/14]

Eurostat (2014). Public procurement electronic systems 2013. http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/dataset?p_product_code=ISOC_CIEG_PEP [08/03/14]

Figueiras A.R. (2012). De máquinas y personas. Reflexiones sobre la inteligencia colectiva y las Tecnologías de la Información y la Comunicación (TIC). *Telos, Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad* (92). Fundación Telefónica España. http://telos.fundaciontelefonica.com/DYC/TELOS/REVISTA/Autoresinvitados_92TELOS_AUTINV1/seccion=1214&idioma=es_ES&id=2012071611570001&activo=7.do [03/03/14]

Gardenal, F. (2010). Public e-Procurement: define, measure and optimize organizational benefits. 4th International Public Procurement Conference, Seúl, Corea del Sur, 26-28 agosto 2010. http://www.ippa.org/IPPC4/Proceedings/05e-Procurement/Paper5-1.pdf [25/02/14]

Gimeno Feliu, J.M. (2011). ¿Hacia una nueva ley de contratos públicos? Observatorio de Contratación Pública, 25/07/11. http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.16/relcategoria.121/relmenu.3/chk.b91d8892df0b2e3d2b56736389f34e91_[03/03/14]

González Alonso, A. (2009). La contratación pública electrónica. *Cuadernos de Derecho Público* (37), 139-175. http://revistasonline.inap.es/index.php/CDP/article/view/9856/10068 [25/02/14]

González, E., Rodríguez, I. (2013). El impacto de la contratación pública electrónica en las PYMES. *Contratación electrónica en el sector público español. Eficiencia, ahorro, transparencia*. http://spain.vortal.biz/files/vortal_es/pdfs/131015_CONTRATACION_ELECTRONICA_EN_EL_SECTOR_PUBLICO_ESPANOL.pdf [09/03/14]

Joongi, K. (2006). National Integrity Systems. Transparency International. Country Study Report. Republic of Korea. http://csis.org/images/stories/hills/06Korea_NationalIntegritySystems.pdf [25/02/14]

Kartiwi, M. (2006). Customer characteristics influence on online trust in developing countries: an examination of conficence level. 6th International Business Information Management Association (IBIMA) Conference, Bonn, 19-21 junio 2006. http://ro.uow.edu.au/commpapers/465/ [08/03/14]

Marques, M.A., Medina, S.A., de Oliveira, A. (2014). Pregão Eletrônico e Eficiência nos Gastos Públicos Municipais. *Administração Pública e Gestão Social* 6 (2) 74-81.

Moreno Molina, J.A. (2011). Prólogo. En Jaime Domínguez Macaya (2011): *Claves para una contratación pública electrónica eficaz*. Madrid: *La Ley*.

Neupane, A., Soar, J., Vaidya, K. (2012a). Evaluating the anti-corruption capabilities of public e-Procurement in a developing country. *The Electronic Journal on Information Systems in Developing Countries*, 55 (2) 1-17. http://eprints.usq.edu.au/22163/1/Neupane_Soar_Vaidya_EJISDC_2012_PV.pdf [25/02/14]

Neupane, A., Soar, J., Vaidya, K. Yong, J. (2012b). Role of e-procurement technology to reduce corruption in government procurement. 2012 International Public Procurement Conference, Seattle, Washington, 17-19 agosto 2012. https://eprints.usq.edu.au/21914/1/Neupane_Soar_Vaidya_Yong_PV.pdf [25/02/14]

Panda, P., Sahu, G., Gupta, P. (2010). Promoting Transparency and Efficiency in Public Procurement: E-Procurement Initiatives by Government of India. 7th International Conference on E-procurement (ICEG), IIM Banglore, India, 20-24 abril 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1880050 [09/03/14]

Pintos, J. (2014). Inmediatez y régimen transitorio de la implantación obligatoria de la contratación pública electrónica en las nuevas Directivas sobre contratación pública. *Contratación Administrativa Práctica* 14 (129), 56-65.

Ramió, C. (2013). Balance del impacto de las crisis económica, política, social e institucional sobre las administraciones públicas en España 2011-2013: Diagnóstico y propuestas. *GIGAPP Estudios Working Papers.* http://www.gigapp.org/es/component/jresearch/?view=publication&task=show&id=937#.UxuFs_l5OSo [08/03/14]

Rodrigues de Faria, E., Marques, M.A., Maia, L., Ramos, S. (2010). Fatores determinantes na variação dos preços dos produtos contratados por pregão eletrônico. *Revista de Administração Pública* 44 (6), 1405-28.

Romeu, J., Juárez, G., Pineda, C. (2014). La contratación pública electrónica como medio para hacer efectiva la transparencia administrativa. *Revista de Estudios Locales* (168), 52-74.

Surowiecki, J. (2004). *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. New York: *Random House.*

Tolbert, C.J., Mossberger, K. (2006). The Effects of E-Government on Trust and Confidence in Government. *Public Administration Review* 66 (3), 354-369.

Vaidya K. (2009). *Electronic Procurement: Impact on Procurement Performance*. Köln: *Lambert Academic Publishing*.

Vidorreta, E. (2013). Análisis de las medidas de impulso para la implantación de contratación electrónica. Observatorio de Contratación Pública, 25/11/13. http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.122/relcategoria.208/relmenu.3/chk.cc824e27040b6b590edc713864a588a1 [08/03/14]

LOS LÍMITES A LA TRANSPARENCIA DE LA ADMINISTRACIÓN PÚBLICA ELECTRÓNICA EN LA ERA DIGITAL

Belén Andrés Segovia
Doctoranda en Derecho Administrativo,
Universidad de Valencia

RESUMEN: Este artículo analizará la reciente Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. La novedad en su implantación, hace que los numerosos profesionales y estudiosos del Derecho, vean en la misma, una oportunidad, para replantear la idea tradicional de la Administración. En todo caso, ya no sólo se trata de garantizar el derecho a la utilización de los nuevos métodos tecnológicos sino también preservar el derecho al libre acceso a la información administrativa que regula la Ley.

PALABRAS CLAVE: Transparencia, administración electrónica, *open data*, tecnología, Derecho Administrativo, política, democracia.

ABSTRACT: This paper deals with the new Act on Transparency 19/2013, of December 9th Act. Such new situation forces both legal practitioners and scholars to reformulate the traditional vision of the public Administration. The enforcement of this Act must guarantee not only the night to use the latest technological methods, but also to preserve the right to a free access to the administrative reformation regulated by the Act.

KEYWORDS: Transparency, e-Administration, open data, technology, Administrative Law, politics, democracy.

1. LA EFICACIA DE LA ADMINISTRACIÓN ELECTRÓNICA

Desde hace ya bastantes años, la sociedad asiste a una serie de cambios en la forma de entender a la Administración. Una nueva forma de percibir las relaciones comerciales, laborales[1], personales y, desde luego, jurídicas, caracterizada por una ruptura con las nociones del tiempo y del espacio. A los ciudadanos, ya no les basta con la existencia de

1 El avance que se produce en la generalización de las nuevas tecnologías e internet, en el ámbito empresarial permite cambiar el modo en que se relacionan con otras empresas, con sus proveedores y con sus clientes, de modo que les facilitan el acceso a los más diversos sectores de actividad profesional y personal. Y es que son muchas las empresas, que utilizan los medios informáticos y telemáticos a fin de crear, unos nuevos mercados virtuales, con unos costes de

servicios públicos, sino que piden y demandan calidad y eficacia[2] en la prestación del mismo. Es esa misma eficacia la que justifica la actuación de la Administración Pública, tal como garantiza el artículo 103 de la Constitución Española (en adelante CE) cuando menciona que «*La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho*»[3].

La regulación legal de la incorporación de los medios informáticos y telemáticos en los diversos sectores de la actividad profesional y personal de la Administración, encuentran su punto de partida en los artículos 38, 45 y 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJPAC). En este contexto tecnológico, la Administración Pública pretende consolidar sus bases de forma que favorezca a sus relaciones con los ciudadanos, de una forma ágil y económica, accesible desde cualquier lugar y en cualquier momento, donde lo importante no es la propia organización administrativa por áreas competenciales, sino la organización por necesidades[4].

La influencia de la técnica, y en particular de las nuevas tecnologías se refleja en todo el sistema jurídico, en particular en el ámbito del Derecho Público. Esa cristalización legislativa de las pautas de adaptación del procedimiento administrativo a las tecnologías de la información y comunicación, con claras aspiraciones de estabilidad tras los años de tanteo que la Administración española ha dedicado al manido asunto de la Administración electrónica y su paulatina integración[5], tiene su reflejo en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios

---

acceso muy bajos, que atraen a un gran número de compradores y vendedores, y automatizan las transacciones.

2 El principio de eficacia es un mandato constitucional de difícil precisión. Prueba de ello, es que el Tribunal Constitucional, en algunas ocasiones, hace referencia al mismo de una forma diferenciada, tal como aluden las sentencias 25/1995, de 21 de enero, FJ 2º, o la 102/1995, de 26 de junio, FJ 31º.

3 Su trascendencia es tal, que el Tribunal Constitucional afirma en la sentencia 27/1987, de 27 de febrero en su Fundamento Jurídico 2º, que tal eficacia no ha de predicarse únicamente de la Administración, sino de todos los poderes públicos, aunque sólo respecto a la Administración está expresamente reconocido.

4 CRESPO RODRIGUEZ, M., en el libro Coordinado por MATEU DE ROS, R. y LÓPEZ-MONÍS GALLEGO, M. (2003)*; Derecho de Internet (La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico),* Thomson Aranzadi, Navarra, p. 704.

5 BOIX PALOP, A. (2007) en su Blog *La Página Definitiva, Derechos de los ciudadanos y neutralidad tecnológica*, publicado el 26/09/2007. *http://www.lapaginadefinitiva.com/aboix/?p=109#more-109.* Fecha de búsqueda: 09/03/2014, 13:56 p.m.

Públicos (en adelante LAECSP)[6] aprobada por el Parlamento, a fin de concretar, los diferentes parches legislativos que rodeaban la materia[7]. A estos efectos, la relación de los avances tecnológicos con el derecho, vienen marcados por esta Ley que prevé según la Exposición de Motivos la necesidad de que «*una Administración a la altura de los tiempos en que actúa tiene que acompañar y promover en beneficio de los ciudadanos el uso de las comunicaciones electrónicas*»[8], al cual cabría añadir el reconocimiento del derecho a la buena Administración, como un derecho fundamental en el ámbito de la Unión Europea[9], con ecos normativos en España[10].

La aplicación de los nuevos métodos tecnológicos da una visión, de la forma de entender a la Administración, que no se oxida ante las novedades técnicas. Con la misma, ya no se persigue únicamente, ofrecer un servicio al ciudadano, facilitando sus relaciones con la Administración de una forma más eficaz, sino que los medios digitales, se han convertido en una norma en muchos procedimientos administrativos, dejando de ser únicamente una dádiva en favor del ciudadano, para ser beneficio también de los poderes públicos que invierten en los medios técnicos y en la formación del personal administrativo, a fin de agilizar el proceso, obteniendo como resultado un gran rendimiento y mejorando su eficacia.

---

6 Publicado en el «BOE» núm. 150, de 23 de junio de 2007, páginas 27150 a 27166 (17 págs.), Referencia: BOE-A-2007-12352. *http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf*. Fecha de búsqueda: 09/03/2014, 13:48 p.m.

7 La LAECSP, pretende sustituir los artículos 38, 45 o 59 de la Ley 30/1992 que se dedicaban a la cuestión, ya que dichos preceptos quedan completados y desarrollados por la nueva Ley, que pretende establecer un marco completo para el empleo de medios electrónicos en las relaciones tanto de los ciudadanos con la Administración como interadministrativas, completando las disposiciones ciertamente parcas.

8 Exposición de Motivos de la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* BOE-A-2007-12352. *http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf*. Fecha de búsqueda 09/03/2014, 14:10 p.m.

9 Base de Datos EURLEX (2010), du document: 15/12/2010, d'envoi: 15/12/2010; *transmis au Conseil Communication de la Commission au Parlament Européen et au Comité des Régions. Plan d'action européen 2011-2015 pour l'administration en ligne Exploiter les TIC pour promouvoir une administration intelligente, durable et innovante/* COM/2010/0743 final */*. Fecha de búsqueda: 09/03/2014. Enlace de búsqueda: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0743:FR:NOT*

10 Tal y como menciona, por ejemplo, en razón de la Ley Orgánica 1/2006, de 10 de abril, de Reforma de la Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana, el artículo 9. 1º cuando dispone que «una Ley de Les Corts regulará el derecho a una buena Administración y el acceso a los documentos de las instituciones y Administraciones públicas valencianas».

En este escenario, el ciudadano deja de ser un mero espectador de la actuación de la Administración, en calidad de usuario, para poder ser un verdadero coprotagonistas en su gestión. La regulación legal sujeta a este análisis, ha supuesto un problema para el usuario en cuanto los procedimientos administrativos electrónicos devienen obligatorios, tal y como muestra la Exposición de Motivos de la LAECSP[11], es decir, cuando no se logran trasladar a los procedimientos electrónicos todas las garantías jurídicas del regulado por la ley del procedimiento administrativo común o cuando se regulan o articulan de forma que la situación jurídico-procedimental del interesado es sustancialmente diferente según si la vía empleada es la presencial tradicional o la electrónica. Para sufragar estas deficiencias la ley ha sido objeto de desarrollo legal en el ámbito estatal a través de una norma reglamentaria, de carácter general, como es el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la LAECSP.

Ambas se tratan de dos herramientas técnicas necesarias para hacer efectivas buena parte de las previsiones de la LAECSP, para la satisfacción de los ciudadanos en cuanto a sus derechos reconocidos a la hora de relacionarse con las Administraciones Públicas por medios electrónicos[12], y por lo que varios años después, resultará llamativa la proliferación de nuevas normas reguladoras de la Administración Electrónica[13]. Pese a los avances normativos que se han producido en los últimos años entorno a la Administración Electrónica, se puede afirmar que no han sido suficientes para solventar las deficiencias normativas sobre las que se ha construido la Administración electrónica, ya que la pluralidad de normas que regulan la materia son el resultado de importantes

11 Exposición de Motivos I, de la LAECSP «*La causa en buena medida se debe a que las previsiones de los artículos 38, 45 y 59 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común son facultativas. (…) Por ello esta Ley pretende dar el paso del «podrán» por el «deberán»*». Enlace: *http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf*

12 Más allá de su trascendencia tecnológica, obedece más bien a que «el contenido de este Real Decreto y sus opciones de política normativa constituyen una clara fuente de inspiración para otras Administraciones Públicas a la hora de dictar sus propias disposiciones sobre la materia» en GAMERO CASADO, E.; *Objeto, ámbito y principios generales de la Ley de Administración Electrónica: su posición en el sistema de fuentes*, en GARMERO CASADO, E., VALERO TORRIJOS, J. (coords.) (2010), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos,* 3ª ed., Thomson-Aranzadi, Madrid, p. 131.

13 Ministerio de Hacienda y de las Administraciones Públicas (2014), *Informe presentado al Consejo de Ministros de 10 de enero de 2014 sobre el grado de avance de la implantación de la administración electrónica en la Administración General del Estado*. Pero la Administración Electrónica para un adecuado desarrollo requiere también la existencia de normas y disposiciones que den validez jurídica y procedimental a sus actuaciones. Desde el año 2011 se han publicado distintas normas que han ayudado a un desarrollo más legítimo, reglamentado y de garantía de la Administración Electrónica.

inconvenientes y disfunciones en su aplicación. Estas irregularidades se producen hasta el punto en que el exceso de regulación hace que la tecnología no pueda desarrollar con seguridad su potencial innovador en el ámbito de las Administraciones Públicas, debido a su exceso de rigidez y una falta de eficacia a la hora de dar respuesta a las necesidades del ciudadano usuario de las redes.

2. EL PAPEL DE LA TRANSPARENCIA EN LA MODERNIZACIÓN ELECTRÓNICA DE LAS ADMINISTRACIONES PÚBLICAS

La configuración legal de la LAE, en relación con los nuevos avances de la tecnología hasta este punto, demuestra la falta de estímulo de una nueva Administración Pública más democrática adaptada a los nuevos tiempos[14]. Una de las principales objeciones que se le puede reprochar a la misma desde el punto de vista de la innovación tecnológica, es la falta de un planteamiento avanzado que permita el acceso a la información. Un modelo de *open data*, que podrá servir para fortalecer a la Administración en su carácter democrático, desde la perspectiva de la *transparencia administrativa*[15]. La clave de la necesidad de innovación del gobierno en cuanto a la transparencia se hace patente debido a que la misma dispone de:

a) En primer lugar, una amplia disponibilidad de herramientas de Internet que permite facilitar el acceso a los datos públicos que hace que el impacto y la necesidad de transparencia sea mucho mayor. Basta pensar en algunas plataformas de publicación gratuitas, tales como blogs, Google Earth, herramientas de visualización, además de todo el software libre y de códigos abiertos que se utilizan en los proyectos Web 2.0.

b) En segundo lugar, la transparencia antes, era un instrumento del que podían disponer los ciudadanos individuales frente al gobierno, y esto limita el impacto de la información obtenida. En la actualidad, lo primero que hace un ciudadano cuando pide información sobre una solicitud, en relación con el principio de Libertad de Información, se encuentra con que los datos reseñados están a su libre disposición en la página web correspondiente.

---

14 En relación a este precepto encontramos el artículo de VALERO TORRIJOS, J. (2012), «El acceso y la reutilización de la información administrativa. Implicaciones jurídicas del proceso de modernización tecnológica de las Administraciones Públicas en su actual y futura configuración», Diario La Ley, núm. 7800.

15 OSIMO, D, (2008), *Benchmarking eGovernement in the Web 2.0 era: what to measure and how», European Journal of ePractice*, núm. 4, p. 6. La transparencia del Gobierno no es en absoluto un tema nuevo. Ha sido el tema de la acción política durante tres siglos. Las primeras leyes sobre el acceso a los documentos públicos se llevaron a cabo en el siglo XVIII en Suecia. Durante los últimos 20 años, la mayoría de los países de la OCDE han adoptado *¨leyes de libertad de información¨* que permitan el acceso a los documentos públicos como un derecho fundamental.

El problema que la misma muestra, es la incertidumbre de sus propios objetivos. Frente a las infinitas posibilidades que ofrecen las nuevas tecnologías, no se incrementa por la ley de forma perceptible la transparencia en el acceso a la información administrativa, ni por lo tanto la participación ni la colaboración con la misma, ya que la transparencia es la premisa inexcusable para estos dos principios. Como enfatiza Osimo, «*la transparencia puede ser no sólo un catalizador para el Gobierno electrónico sino, además y sobre todo, un dinamizador de la transformación en el ámbito del sector público en su conjunto*». Con el fin de solventar estas deficiencias, el legislador crea la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[16] (en adelante LT). Con esta ley se pretende: en primer lugar, *incrementar y reforzar la transparencia* de la actividad de las Administraciones Públicas; en segundo lugar, reconocer y garantizar el *acceso a la información pública* solicitada por los usuarios; y en tercer lugar establece las *obligaciones de buen gobierno* que la nueva regulación llevará a cabo los responsables públicos y las consecuencias jurídicas que el incumplimiento de su aplicación implica[17].

2.1. Reforzar e Incrementar la Transparencia

La LT profundiza en la configuración de la *publicidad activa* (art. 5); a través de la cual «*publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública*». Se crea a manos de la Administración del Estado un *Portal de Transparencia* que impone la publicación «periódica y actualizada» de Planes, actuaciones, resultados e información de *relevancia jurídica* que cuando menos, será la contenida en los artículos 6, 7 y 8 de la Ley.

El problema jurídico que se plantea en este ámbito en primer lugar es la precisión con la que se mide el criterio por el que se determina si un suceso *es o no relevante jurídicamente* y en segundo lugar la falta de un criterio que determine la *periodicidad* por las que se deberán regir las publicaciones, a fin de seguir una coherencia expositiva, garantizar de forma plena la transparencia. A su vez, la publicación de un organigrama que muestre un parco y discreto currículum de dichas autoridades, por el que no es preceptivo que se muestre como fue llevado a cabo su nombramiento, o la falta de expresión

16 Publicado en el BOE núm. 295 de 10 de Diciembre de 2013. Fecha de búsqueda: 09/03/2014, 20:57 p.m.

17 La reciente Ley de transparencia defiende en su Exposición de Motivos que «*la transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamentales de toda acción política*»; palabras cuyo significado en cierta medida se desvanece una vez se analiza pormenorizadamente el contenido de la misma.

de si figura en el mismo alguna causa de ilegalidad, no garantiza otra cosa más que la opacidad con la que se pretende llevar a cabo este precepto.

También dice la Ley, que la misma deberá vincular a un gran número de sujetos entre los que se encuentran las Administraciones Públicas, los órganos del poder Legislativo y Judicial en lo que se refiere a sus actividades sujetas a Derecho Administrativo (art. 2.1.f) LT), así como los órganos constitucionales y estatutarios. Asimismo, se aplicará a determinadas entidades, que por su especial relevancia pública, o por su condición de preceptor de fondos públicos, precisen reforzar su grado de trasparencia.

En este contexto, quedan fuera de su regulación el contenido de sus funciones ya que sólo se alcanza las actividades sujetas a Derecho Administrativo. También queda fuera de esta casa de transparencia sus actividades dentro del Derecho Privado tales como contratos privados, personal laboral, bienes patrimoniales, etc. A su vez, se proyecta sobre «*los partidos políticos, organizaciones sindicales y organizaciones empresariales*» (art. 3.1.a) LT), pero no a las entidades vinculadas o dependientes de la mismas, ya sean bien sociedades mercantiles, fundaciones u otro tipo de entidades.

Además, se tendrán en consideración a los efectos de dar transparencia a las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40% del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros (art. 3.1.b) LT), pero no se prevé por la misma la duplicidad de entidades privadas, aparentemente distintas, a fin de burlar dichos porcentajes.

2.2. Derecho de acceso a la información pública

Es importante, en primer lugar, identificar las técnicas de control de las actividades administrativas difusas e indirectas[18]. El principio de transparencia de las actuaciones de la Administración Pública presentes en el artículo 105.b CE[19] y regulada con carácter general en el artículo 37 de la Ley 30/1992[20], adolecen de una serie de deficiencias al

18 El derecho de acceso a la información pública se puede comparar una casa de cristal, a través de la cual se puede ver lo que hay en su interior, pero con un armario, que no deja ver con claridad su contenido, al reducirse a documentos que se encuentran contenidos en procedimientos administrativos ya terminados, y al resultar su ejercicio limitado en su articulación práctica.

19 El artículo 105.b) en relación con el principio de acceso, hace referencia a que, «*la ley regulará: El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas*», es decir, el derecho de los ciudadanos al acceso a los archivos que almacena la misma.

20 El legislador desarrolla el derecho del artículo 105.b) años después de la Constitución mediante la aprobación del artículo 37 de la LRJPAC. Se trata de un artículo extenso, plagado de ex-

no mostrarse con claridad la delimitación del concepto correspondiente al derecho de acceso a la información pública, también previsto en el art. 13 LT.

La LT en este aspecto, permite conocer cualquier expediente administrativo que se desee consultar, sin necesidad de motivación para llevar a cabo dicha solicitud. El procedimiento sería el siguiente: en primer lugar, se procede a la solicitud y la Administración dispone de un mes para resolver (art. 20.1 LT). En segundo lugar, se prevé el silencio administrativo desestimatorio al caso de la falta de resolución en el plazo de un mes a la solicitud de información (art. 20.3 LT) y, de nuevo, un silencio desestimatorio al caso de que el Consejo de Transparencia y Buen Gobierno no resuelva por lo que cabe la reclamación potestativa (art. 20.5 LT) y recurso previo a la vía judicial en plazo de tres meses (art. 24.4 LT). De nuevo habrá que recurrir a la vía judicial, con todas sus consecuencias, para el ejercicio de nuestros legítimos derechos de información, pagando las tasas judiciales y con una exposición a la imposición de las costas, resultando en muchos casos, poco rentable el llegar hasta sus últimas consecuencias. En este contexto resulta inaceptable que una Administración Pública, que debe actuar «con sometimiento pleno a la Ley y al Derecho» (art. 103.1 CE), desatienda, primero, sus obligaciones con los ciudadanos de acuerdo con la figura del silencio y, sin embargo, exprese un mayor celo en el momento de exigir su cumplimiento, pues ninguna pretendida eficacia administrativa puede justificar el desconocimiento de unos de los valores superiores de nuestro Ordenamiento jurídico, como el valor justicia (art. 1.1 CE). Por este motivo, tal y como se ha pronunciado la Sentencia de la Sala Segunda Tribunal Constitucional 14/2006, de 16 de enero[21], no es posible entender, que la resolución desestimatoria presunta de un recurso potestativo, como es el de reposición, por *silencio administrativo de carácter negativo* regulada en el artículo 43.2 de la LRJPAC[22] reúna, los requisitos formales de que se debe revestir todo acto administrativo, por el simple hecho de que el acto impugnado

cepciones y prohibiciones, en el que destaca la falta de una regulación en positivo, y que viene acompañado de múltiples excepciones, que conducen a la aplicación de una regulación específica, a fin de conocer su contenido. Dos ejemplos de corte restrictivo de este artículo 37 serían: en primer lugar, los documentos nominativos, se encuentran fuera del derecho de acceso a la información, de acuerdo con el principio de transparencia, y en segundo lugar, no se permite ejercer este derecho más que si el Estado identifica concretamente la información solicitada por el usuario. Además en esta línea, se puede denegar o retrasar el acceso, de forma que se ve perturbado el funcionamiento de la oficina administrativa.

21 Sentencia de la Sala Segunda del Tribunal Constitucional 14/2006, de 16 de Enero (RTC 2006\14).

22 Según el artículo 43.2 de la LRJPAC, «La estimación por silencio administrativo tiene a todos los efectos la consideración de acto administrativo finalizador del procedimiento. La desestimación por silencio administrativo tiene los solos efectos de permitir a los interesados la interposición del recurso administrativo o contencioso-administrativo que resulte procedente».

sobre el que pende la inactividad administrativa[23] incluyó una detallada instrucción de recursos, presentes y futuros.

2.3. Buen Gobierno

El Consejo de Transparencia y Buen Gobierno se crea a fin de promover la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de publicidad, salvaguardar el ejercicio de derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno (art. 33). Un órgano «*imparcial*»[24] formado por representantes de los propios órganos y entes administrativos a controlar, además de su configuración mayoritariamente política, que recaerán en «*personas de reconocido prestigio y competencia profesional*», concepto de difícil determinación, cuya determinación recae sobre el Consejo de Ministros (art. 37.1 LT).

2.4. Las insuficiencias de la Ley de Transparencia

Pese a la consideración de que la nueva regulación, a través de la Ley de Transparencia es más completa y sistemática que su predecesora y, en última instancia, puede servir como un revulsivo para favorecer el acceso a la información en poder de las Administraciones Públicas, lo cierto es que su concepción muestra una serie de insuficiencias que no podemos eludir.

En materia de *transparencia activa*, –capítulo II del título I–, si bien desde el punto de vista de la innovación tecnológica su planteamiento es limitado, el grado de obligatoriedad en el cumplimiento es importante a los efectos de reforzar y mejorar su regulación[25]. La consideración de la Ley de Transparencia es a estos efectos bastante generosa desde el punto de vista legislativo, tanto para las Comunidades Autónomas, como para los diferentes Entes Locales. Pese a ello se crea un punto de inflexión en cuanto a la in-

23 Así, la Sentencia del Tribunal Supremo de 13 de Abril de 2011 (rec.3519/2009); Sentencia del Tribunal Supremo de 28 de febrero de 2007 (rec.302/2004); STS Justicia de Galicia de 8 de Febrero de 2012 (rec.265/2011); y la Sentencia del Tribunal Supremo en la Sala de lo Contencioso de 8 de Enero de 2013 (rec.2/2013).

24 Un órgano «supuestamente» imparcial y decimos bien, supuestamente, una vez que comprobamos que estará formado por representantes de los propios órganos y entes administrativos a controlar. Un ejemplo ilustrativo del mismo sería, cuando la ilegalidad sea cometida por un Alcalde, quien deberá controlar su actuación será el mismo. Bajo esta premisa podemos observar que esta medida queda lejos de ser objetiva.

25 VALERO TORRIJOS, J., (2014), «Ley de Transparencia, bien pero…» En el blog jurídico «Derecho, Tecnología y modernización administrativa» Fecha de publicación: Jueves, 13 de febrero de 2014. Fecha de búsqueda: 10-05-2014, 1.39 a.m.

certidumbre en su regulación y sucesiva aplicación por los portales de transparencia ante un posible incumplimiento de la misma.

A estos efectos, la LT se declara insuficiente, por lo tanto, falta de una regulación más completa y exhaustiva de sus preceptos. Es decir, esto se debe a que pese a que se percibe una cierta mejora en la misma, no se prevé un sistema sancionador claro ante el posible incumplimiento de las Administraciones con todos y cada uno de los criterios asignados a los portales de transparencia y que a su vez conlleve la correspondiente sanción que considere necesaria. Al respecto y a fin de difuminar dicha insuficiencia, se pronuncia el artículo 29 de la Ley de Transparencia por el que se impone que, en el caso de que se suceda el incumplimiento reiterado de las obligaciones de publicación activa podrá ser considerado *infracción grave* y podrá considerarse la responsabilidad disciplinaria contemplada con carácter muy limitado –artículo 9.3 LT–, cuya aplicación se llevará a cabo en relación con la publicidad activa y no por lo que se refiere al incumplimiento de la obligación de resolver.

Llegados a este punto encontramos dos frentes; en primer lugar, *la posibilidad de que las Comunidades Autónomas acaten estas medidas* y lo regulen en su derecho sancionador autonómico dejando claro quiénes serían responsables, plazos a cumplir y lo que sucederá ante un posible incumplimiento. Y en segundo lugar, las Comunidades Autónomas que posiblemente de forma mayoritaria, *no acaten de forma estricta cada uno de los preceptos reseñados en la normativa de transparencia*, a través del cual repetirán la normativa estatal. En tal caso, ante su incumplimiento no verán necesario realizar su obligación activa, donde la idea que se plantea, entre otras cosas, de que el derecho sancionador de la administración no ha sido objeto de un funcionamiento óptimo, es una amenaza que siempre puede servir, al menos a fin de concretar que unidades administrativas son responsables de hacer cumplir la ley.

Son varias las Comunidades Autónomas que siguen esta línea por ejemplo, el primer portal de regulación autonómica fue el de Cataluña[26]. Con el transcurso del tiempo se han incorporado otros territorios como es el caso de la Comunidad Valenciana, donde su aprobación se anunció en diciembre, pese a disponer de una versión muy reducida de la misma ya que su intencionalidad era una aplicación más básica. Esta opción hace probable, que no se cumpla con todos los puntos de exigencia (como sería el caso en materia de contratación y convenios donde la posibilidad de su cumplimiento es bastante difícil de gestionar). Esta medida es un primer paso para poder *hacer público algunos datos personales de los políticos*, sin perjuicio de que sea un somero relato sobre informaciones de los mismos que no les comprometan en

26 Véase en el Parlament de Catalunya «Proposició de llei de transparència, accés a la informació pública i bon govern» *http://www.parlament.cat/actualitat/ects/resum_transparencia.pdf*. Fecha de visita: 10.05.2014, 11.47. En Fase de Tramitación.

exceso[27]. Por lo tanto, la mayoría de Comunidades Autónomas estarán a la expectativa de la actuación del Estado, y de este modo poder seguir un modelo semejante que analizará hasta qué punto pueden cumplir con las obligaciones de información a través de su página web o portal de internet. Otra cuestión que no queda resuelta en este sentido, es si la publicación en Boletines Oficiales responde a la voluntad de transparencia, con el objeto de dar a conocer una información a la generalidad de los ciudadanos, para posibilitar el conocimiento y control de la actuación pública. Al respecto se refiere el artículo 3.5. LRJPAC que regula el principio de participación junto al de transparencia en el artículo 37 LRJPAC y prevé al respecto en sus artículos 59.6 LRJPAC y 60 LRJPAC, supuestos legales de publicación sustitutoria[28] en Boletines Oficiales. Cabe plantearse al respecto, si es preciso mantener la publicación de estos datos en boletines oficiales, en lugar de hacerlo en sedes electrónicas de los respectivos organismos, o en su caso, en un portal de transparencia centralizado de cada Administración o del conjunto de ellas. Sin embargo, la tendencia no es hacia su publicación en los diarios oficiales, sino en algunas páginas webs oficiales. A ello cabe añadir, que internet no es en sí misma, una fuente de acceso público y, por tanto, los datos obtenidos no pueden ser utilizados para una finalidad incompatible con aquélla para la que fueron comunicados. Es de esperar que este asunto se resuelva con una futura norma de transparencia, siguiendo una serie de principios que quedan desarrollados en el Derecho comparado y a su vez son reseñados por la doctrina, que permitan la ponderación entre transparencia y privacidad[29].

Algunos de estos elementos llaman la atención desde la perspectiva relacionada con el derecho a la información pública, con una regulación de carácter general en el art. 105. b) donde ya se reconocía como derecho de todos los ciudadanos el acceso a todos los archivos y registros públicos «*salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas*». Este derecho sí que ha sido considerado desde una perspectiva subjetiva, del derecho naciente o nacido en este proceso. El objeto de esta ley puede decirse que es cambiar todo para que nada cambie. No es una ley novedosa, y no es que sea la última ley que recoja lo mejor de las anteriores regulaciones, es más bien una ley media, pero a su vez bastante razonable, siendo desde el punto de vista jurídico bastante seria en algunos aspectos pero criticable en otros.

---

27 COTINO HUESO, L., (2014), «Conferencia Inaugural sobre la Ley de Transparencia», Asociación Profesional Española de Privacidad, Universitat de València, Fecha: 02.04.2014.

28 TOSCANO GIL, F., (2012), «Publicación de actos administrativos y protección de datos de carácter personal» Revista de Derecho Administrativo, núm. 31.

29 GUICHOT REINA, E., (2012), «La publicidad de datos personales en internet por parte de las Administraciones Públicas y el Derecho al Olvido» Revista española de derecho administrativo, núm. 154, pp. 126-127.

La nueva regulación tiene su parte positiva, en primer lugar, desde la perspectiva de que mejora la situación anterior, ya que el artículo 37 de la ley 30/1992 era insuficiente, en relación al tipo de información a la que pueden acceder los ciudadanos a través del ejercicio de este nuevo derecho, pues es toda la información que poseen los poderes públicos cuando realizan funciones públicas. En segundo lugar, es un concepto muy generoso, donde la ley habla de información no de archivos y expedientes, tal y como se concebía en el art. 105.b) de la CE.

Por otro lado, la Ley muestra su escasa regulación en relación a las causas de inadmisión de las solicitudes de los ciudadanos a la información pública. Hay algunas que son razonables y otras que habrá que ver su interpretación. Este sería el caso, de todas las comunicaciones internas, borradores, materiales que se encuentran en fase de gestación y que se excluye de lo que está en fase de acceso a la información. En muchos casos esta regulación será muy importante para el ciudadano a fin de poder acceder a las comunicaciones e informes internos de la administración y de este modo poder saber cuál es el estado en que se encuentran determinados ámbitos sectoriales. En caso de sucederse una inadmisión directa supondría, la ausencia de estudio de su relación a salvaguardar el interés público de acceso a la información, punto en el que la ley ha sido relativamente criticable.

En cuanto a las *causas de restricción* la Unión Europea habla de un listado muy amplio del derecho a la información que desde el primer anteproyecto se ha criticado mucho[30]. En este aspecto, la ley deja claro que se ha de valorar el interés público en el acceso a la información y será el Consejo de la Transparencia u otros órganos judiciales, quienes deban valorar la procedencia del mismo. Una de las grandes ventajas de la ley de transparencia es que los ciudadanos no van a tener la necesidad de acudir a los tribunales, donde lo más probable es que haya decaído su interés años después, de acceder a la información, y darse de este modo el caso de un posible desistimiento por haber perdido su sentido. A fin de evitar la ausencia de protección, la ley hace referencia a la existencia de un órgano que no supone ningún coste para los ciudadanos, opción considerable teniendo como ejemplo una época marcada por el excesivo coste de pleitear objeto de las tasas judiciales. El acceso a este órgano es *potestativo,* siendo este una posible vía a través de la cual el ciudadano podría reclamar sus derechos, es decir, el ciudadano podrá decidir, ante una denegación al acceso de la información, entre si va a la vía judicial, o a esta agencia teóricamente «independiente» que es el Consejo de la Transparencia.

Desde el primer proyecto de ley se optó por un órgano diferente a la Agencia de Protección de datos[31]. Esta opción no suele ser lo habitual pero tampoco es excepcional,

30 DYRBERG, P., (1997), «El acceso público a los documentos y las autoridades comunitarias», en Revista de Derecho Comunitario Europeo, nº 2, vol. I, p. 381.

31 Véase el Boletín General de las Cortes Generales, el «Proyecto de Ley de transparencia, acceso a la información pública y buen gobierno», Fecha de publicación: 07.09.201, núm. 19-1, p.

ya que hay modelos de Agencias Independientes sobre transparencia que son diferentes de las Agencias Independientes para Proteger los Datos Personales, la privacidad y hay modelos en los que lo reúnen todo en el mismo órgano, ejemplo de utilización de esta figura era el caso Mexicano para proteger la transparencia y el derecho a la información, que tuvo como resultado la Ley de Protección de Datos del 2012 donde se incorporan las funciones en materia de protección de datos[32], y en el caso de Inglaterra en que nacen conjuntamente la ley de transparencia que asigna a la Agencia de Protección de Datos[33]. Es decir, son modelos a seguir diferentes, ambos con sus respectivas ventajas y desventajas.

La opción asumida en España en esta materia hasta el momento, ha sido una protección hipertrofiada del derecho de protección de datos. Este órgano tendría que defender un derecho sobre el que no tiene preferencia, por lo que la balanza se inclinaría hacia la protección de datos. Esta regulación no es uniforme, encontramos el ejemplo Cataluña y el País Vasco, donde las Agencias de Protección de Datos van a asumir esta doble función de Protección de datos y Transparencia. En el caso de Andalucía, se va a crear una agencia con la doble función, y en España se da este mecanismo bicéfalo en el que la ley especifica que ambas funciones deberán coordinarse y así poder observar los criterios a seguir en esta materia.

Las garantías del *Consejo de la Transparencia* otorgan a este órgano administrativo una cierta dosis de independencia. La clave va a estar en quien será el responsable de la dirección del mismo. Tal *nombramiento* será el que determinará el correcto e imparcial funcionamiento del Consejo de la Transparencia en un futuro. En caso de que los criterios de ponderación no funcionen correctamente, serán los órganos judiciales mediante sentencia, quienes determinen si se cumplen o no los derechos del ciudadano deman-

---

1. Enlace: http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-19-1.PDF

32 En el Diario Oficial de la Federación. El Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Referencia del Decreto DOF: 05/07/2010. Fecha de visita: 10.05.2014, 14.49 p.m. Enlace: *http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010*.

33 COTINO HUESO, L., (2006), «Transparencia y derecho de acceso a los documentos en la Constitución europea y en la realidad de su ejercicio», en *La Constitución Europea: Actas del III Congreso de la Asociación de Constitucionalistas de España.* Tirant lo Blanch, Valencia, pp. 285-308. El mismo las define como*, «figuras independientes sólo responsables ante los parlamentos –similares al ombudsmen- encargada también en algunos casos –como Reino Unido- de la protección de datos personales, que como sabemos implica también derechos de acceso a la información, y del acceso a la información pública. Así, entre otros, el Information Commissioner del Reino Unido».* Enlace: *http://www.lcd.gov.uk/fol/foldpunit.htm.*

dante. Para concluir, el planteamiento material de estos supuestos ha llegado al Tribunal Supremo. Las resoluciones más recientes al mismo, en 2012 y el Tribunal Constitucional en el 2013, se pronuncian en sentido de que no hay un derecho fundamental objeto de protección pero, tampoco hay que olvidar el dato de que el Tribunal Europeo de Derechos Humanos en su sentencia ultima de agosto no comparte este criterio[34].

3. CONCLUSIÓN

La Ley de Transparencia nace por lo tanto, bajo la vocación de un funcionamiento más eficaz de la Administración Pública en conjunción con el artículo 103 de la Constitución Española. La idea de reforzar el principio democrático bajo los auspicios de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, hace pensar, que el avance tecnológico junto con la revolución de internet, puede llegar a ser el resultado que nos conduzca a un mayor control de la Administración y una herramienta más de lucha contra la corrupción, ante un panorama opaco donde las decisiones políticas, empañan los cristales de la Administración. Hasta hace poco en España no había una cultura de transparencia a diferencia del norte de Europa, como la cultura puritana y la cultura calvinista. Es una materia que ha costado mucho tiempo y sin embargo no mucho dinero. Si la ciudadanía ejerce y utiliza los mecanismos de esta ley será una materia útil. En consecuencia, si la interpretación doctrinal considerase como garante de los derechos fundamentales, la Ley de Transparencia 19/2013 en España, tal y como sucede en Europa, tendríamos un país mucho más transparente.

4. BIBLIOGRAFÍA

Ayala Muñoz, J. (2002); *Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo,* ed. 2º, Aranzadi Editorial, Navarra, p. 316.

Ballester Espinosa, A. (2013); *Administración Electrónica, Transparencia y Open Data como generadores de confianza en las Administraciones Públicas,* Málaga. *http://www.academia.edu/4053866/Administracion_Electronica_Transparencia_y_Open_Data_como_generadores_de_confianza_en_las_Administraciones_Publicas*

Belando Garín, B. (2002); *Nuevas perspectivas del régimen local. Estudios homenaje al profesor José María Boquera Oliver: El silencio administrativo y la inactividad en la nueva LJCA,* Tirant lo Blanch, pp. 1213-1231.

34 VALERO TORRIJOS, J., (2014), «Conferencia Inaugural …», op.cit, Universitat de València, Fecha: 02.04.2014.

Boix Palop, A. (2007); en su Blog *La Página Definitiva, Derechos de los ciudadanos y neutralidad tecnológica*, publicado el 26/09/2007. Fecha de búsqueda: 09/03/2014, 13:56 p.m. *http://www.lapaginadefinitiva.com/aboix/?p=109#more-109*

Cotino Hueso, L. (2007); *Los derechos de los ciudadanos ante la Administración Electrónica,* Universidad de Valencia. http://documentostics.com/component/option,com_docman/task,doc_view/gid,1518/

Crespo Rodriguez, M., en el libro Coordinado por Mateu de Ros, R. y López-Monís Gallego, M. (2003)*; Derecho de Internet (La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico),* Thomson Aranzadi, Navarra, p. 704.

Gamero Casado, E. (2007); *Ventanilla única y administración electrónica en la transposición de la directiva de servicios*, Universidad Pablo de Olavide, Sevilla. http://pagina.jccm.es/ear/repositorio/VENTANILLA_%C3%9ANICA_Y_ADMON_ELECTR%C3%93NICA_EDUARDO_GAMERO.pdf

Gamero Casado, E., Valero Torrijos, J. (coords.) (2010); *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos,* 3ª ed., Thomson-Aranzadi, Madrid, p. 131.

Guichot Reina, E., (2012); «La publicidad de datos personales en internet por parte de las Administraciones Públicas y el Derecho al Olvido» Revista española de derecho administrativo, núm. 154, 2012, pp. 126-127.

Osimo, D., (2008); *Benchmarking eGovernement in the Web 2.0 era: what to measure and how*, European Journal of ePractice, núm. 4, p. 10.

Piñar Mañas, J.L. (Coordinador) (2011); *Administración Electrónica y ciudadanos,* Thomson Reuters, Civitas, Madrid, pp. 289-324.

Rodriguez Seoane, G.J. (2013); Proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno: *Breve comparación del proyecto español con la ley chilena, otras leyes latinoamericanas, y con la realidad europea*, Universidad de A Coruña (UDC).

Toscano Gil, F., (2012), «Publicación de actos administrativos y protección de datos de carácter personal» Revista de Derecho Administrativo, núm. 31.

Valero Torrijos, J.:

— (2007) *La nueva regulación legal del uso de las tecnologías de la información y las comunicaciones en el ámbito administrativo: ¿el viaje hacia un nuevo modelo de Administración, electrónica?,* Departamento de Derecho Administrativo, Universidad de Murcia. *http://www.um.es/deradmv/julivale*

— (2012); *El acceso y la reutilización de la información administrativa. Implicaciones jurídicas del proceso de modernización tecnológica de las Administraciones Públicas en su actual y futura configuración*, Diario La Ley, núm. 7800.

— (2013); *Derecho, innovación y administración electrónica,* Global Law Press, Murcia, pp. 205-401.

COMUNICACIONES SOBRE POLÍTICA E INTERNET

ANONYMOUS BULGARIA: «I LIKE TO LUMPEN LUMPEN»

Julia Rone
PhD researcher, Department of Social and Political Science, European University Institute, Florence

ABSTRACT: The current paper explores the involvement of anonymous Bulgaria in the protests against the Bulgarian government in June, 2013. The paper approaches Anonymous through the prism of anarcho-communist theories of open, horizontal, collaborative networks and asks whether the collective is really open and inclusive and whether such an organization can provide a viable alternative to more institutionalized forms of resistance. In order to assess the political potential of Anonymous Bulgaria, I address three sub-questions: 1. Who are Anonymous Bulgaria and what is their internal structure? 2. What kind of social critique did Anonymous Bulgaria engage in during the period I observed? 3. What kind of alternative social order do Anonymous envisage?

The paper claims that there is no such thing as Anonymous Bulgaria but instead there are multiple loosely connected factions that use the same name for different purposes. While some factions of the group leaked information about corrupt politicians, others targeted NGO representatives and public intellectuals. The general opposition of Anonymous to any form of institution («Fuck the system») led to a state of all-pervading suspicion which was so general that it lost political effectiveness. Based on a politics of unmasking and on an ideology of fluidity and leaderlessness, the operations of Anonymous Bulgaria could not go beyond 'hacking politics' and offer a positive vision of what the protests had to achieve.

KEYWORDS: Anonymous, multitude, horizontality, openness, anarcho-communism.

1. INTRODUCTION: MAFIA OWNS THE GOVERNMENT

'The boulevard is blocked because of the protests. We can't pass by the National Assembly': that was the first thing the taxi driver told me on my way home from the airport. It was the 22nd of June, 2013, day 9 of the peaceful #DANSwithme protests in Bulgaria. The protests started on the 14th of June with the appointment of the controversial media owner Delyan Peevski as the head of the national security agency (DANS). The decision of the three-week old government provoked huge public outrage and thousands of people took to the streets to protest against corruption and the oligarchic mechanisms of power. A popular sign during the protests read: 'The mafia owns the government, whether it owns the people as well depends on us' (fig. 1).

Fig. 1. 'The Mafia Owns the Government'. Source: ANONYMOUS BULGARIA, 2013.

People continued protesting even after the resignation of Peevski with requests for new elections but also for a general change in the electoral system. There were mass demonstrations every single day and a siege of the parliament in July. In October students occupied Sofia University - the biggest and oldest higher education institution in Bulgaria, protesting against corruption and façade democracy. The protests have been losing track but still continue in different forms in 2014.

In the current paper I would like to explore the involvement of Anonymous Bulgaria in the first wave of the anti-government protests in June, 2013. My main research question is: what is the political potential of Anonymous Bulgaria? In order to answer this question I have divided it into three sub-questions: 1. Who are Anonymous Bulgaria and what is their internal structure? 2. What kind of social critique did Anonymous Bulgaria engage in during the period I observed? 3. What kind of alternative social order do Anonymous envisage? All these are empirical questions that can be answered through observation and data collection. But they address a deeper theoretical problem: the idea that open, horizontal, participatory networks that are not based on membership can provide an alternative to the current form of liberal representative democracy (Hardt and Negri, 2005). In this respect, the current paper confronts anarcho-communist theory with empirical observations and analyzes the creative tensions between them. Exploring the actions of Anonymous in the times of anti-government protests in Bulgaria is particularly suitable for this goal as this was a period of vivid social critique and debate in which social actors themselves were constantly asking questions about who they are, what they want and what kind of alternative political orders are possible.

2. THEORETICAL REVIEW: ANOTHER WORLD IS POSSIBLE?

In the current section I would like to explore the genealogy of the Anonymous collective. The history of Anonymous starting from the image boards on *4Chan* and

passing through the stage of massive protests against the Church of Scientology before assuming its current more political form of attacks on government web sites and infrastructure has been already well documented and analyzed (Coleman, 2011; Coleman, 2012; Kelly, 2012). What I would like to do instead is to trace the theoretical underpinnings of the collective and the discourse of openness, horizontality and inclusivity that makes the existence of such a group possible.

To begin with, what are Anonymous? Kelly quotes the definition provided by the group itself: «On its website, Anonymous describes itself as 'an internet gathering' rather than a 'group'. Moreover, Anonymous states that it has 'a very loose and decentralized command structure that operates on ideas rather than directives'» (Kelly, 2012: 1678). In addition, anyone who wants to join Anonymous must know that: «You cannot join Anonymous. Nobody can join Anonymous. Anonymous is not an organization. It is not a club, a party or even a movement. There is no charter, no manifest, no membership fees. Anonymous has no leaders, no gurus, no ideologists. In fact, it does not even have a fixed ideology» (Anon2k13, 2013). In practice, Anonymous consists of hackers and geeks, people with a number of digital literacies united by a common online culture of shared references, jokes and attentiveness towards injustice both online and offline (Coleman, 2011). As the group states in their 2010 press release: «Anonymous is not a group of hackers. We are average Interent Citizens ourselves and our motivation is a collective sense of being fed up with all the minor and major injustices we witness every day» (ANON OPS, 2010). According to Kelly, the key characteristics of the group are: 1) the unrelenting moral stance on issues and rights; 2) a physical presence that accompanies online hacking activity; 3) a distinctive brand (Kelly, 2012: 1680).

The problem with every attempt to define Anonymous is that definitions are totalizing by nature. And with an amorphous gathering such as Anonymous every attempt to provide a definite description borders on inaccuracy. Maybe the best way to define Anonymous is to resist to provide an ultimate definition and to use working definitions open to change as the group itself. The radical openness, fluidity and inclusiveness combined with a general will to be against are what makes Anonymous Anonymous. The problem is: is the group really so open and inclusive? Or are there hidden contradictions, divisions and mechanisms of exclusion? And what is so bad about hierarchies, institutions and stability?

Jordan and Taylor (2004) trace the origins of hacktivism, defined as online direct action, to three different but interlocking contexts: the hacking community, the increasing prominence of immaterial labor and immaterial commodities in contemporary society, and the new social movements. Hacktivism draws in «powerful alternative visions of society, arming these visions with informational tools and injecting itself as a radical virus into twenty-first century societies» (Jordan and Taylor, 2004, 165). Hacktivism is inspired by the «hacker ethics» that appeared in the 1980s and emphasized the value of sharing, access to computers and freedom of information, decentralization and mistrust of authority

(Levy, 1984). These ideas found a convincing expression in the free software movement which proclaimed that free software is a prerequisite for a free society. Richard Stallman was one of the first «hackers» to emphasize the directly political nature of technology. He fought for free software, claiming that «free» is a matter of liberty and not a matter of price: it is «free» as in «free speech» and not as in «free beer» (Stallman, 2002). A program is free software if the program's users have the four essential freedoms: to run free the program, to study how the program works and change it, the freedom to redistribute copies and the freedom to distribute modified copies to others (What is Free Software, 2013).

And while Stallman insists on the politics of technology, political theorists such as Hardt and Negri use technology as a metaphor that allows them to propose a new vision of politics: they propose a society «whose source code is revealed so that we all can work collaboratively to solve its bugs and create new, better social programs» (Hardt and Negri, 2004, 340). The faith in participation, collaboration and openness is common both to the techno-geeks and the anarcho-communist political theorists. From the standpoint of sociology of critique, Luc Boltanski traces the suspicion towards any institutions and forms of hierarchy to the relational philosophy of Delezue and to the social movements of the 1960s when young people rebelled against Fordist wage regimes, Taylorist methods of labor organization and a paternalistic welfare state. The so-called new social movements developed since the 1960s on issues such as gender relations, environmental protection, peace and international solidarity and had a strong middleclass basis in contrast to earlier working-class or nationalist collective action (Della Porta and Diani, 2006: vii). Boltanski claims that the emphasis on freedoms and the right of individuals to determine their identity forms part of a critique which might be labelled «artistic» and which was successfully incorporated by the spirit of capitalism to give birth to a culture of projects, networking and constant mobility. However, the social critique aimed at redistribution and social justice was neglected and suppressed (Boltanski, 2005).

Writing in the 1990s and 2000s Hardt and Negri provide a good example of the artistic critique of capitalism, focusing on the emancipator power of mobility, freedom and individual difference. They offer a useful synthesis of the story both of the rise of a new biopolitical form of production and the resistance against it, of Empire and the multitude. Their bestselling book «Empire» is a timely response to Fukuyama's notion of the end of history. Capitalism has transcended all national borders and prevailed around the world creating an integrated global market, a new world order in which economic production and political constitution tend increasingly to coincide. Empire is not a particular nation state or a supranational entity. Empire is a machine, a mechanism for producing goods but also subjectivities, ideas, affects and social relations. The authors talk about the succession of different economic paradigms: from primary production (agriculture and extraction of raw materials) to secondary production (industry and manufacture of durable goods) to tertiary production (services and manipulating information). It is precisely this passage from the secondary to the tertiary economy which

they call postmodernization or even better: informatization (ibid, 280). And since the production of services does not result in a tangible, material good, the notion of immaterial labor is introduced – «labor that produces an immaterial good, such as a service, a cultural product, knowledge and communication» (ibid, 290). The key point in the argument is that we all «participate in a productive world made up of communication and social networks, interactive services, and common languages...Producing increasingly means constructing cooperation and communicative commonalities» (ibid, 302).

So, on the one hand, there is the global proletariat, a multitude of individuals no longer constrained by national boundaries, individuals constantly on the move who are becoming entangled in denser and denser networks of cooperation, and on the other hand, there is Empire that extracts as a parasite the value produced by these individuals. The main argument of Hardt and Negri is that there is no way back. The traditional left with its insistence to protect the local and the welfare state is fighting for a lost cause. What is needed to win against Empire is more globalization, more mobility, more deterritorialization. Hardt and Negri remind us of the original impulse of internationalism and the notion that the proletariat «has no country», that «the country of the proletariat is the entire world» (ibid, 49). So not only has capitalism become all-pervasive, but also the notion of «proletariat» has expanded and acquired new dimensions to encompass all those exploited by and subject to capitalist domination. Yet this should not indicate that the proletariat is homogeneous or undifferentiated: «It is indeed cut in various directions by differences and stratifications» (ibid, 53). Or to quote sub-comandante Marcos from the Zapatista movement: «Marcos is gay in San Francisco, black in South Africa, an Asian in Europe, a Chicano in San Ysidro, an anarchist in Spain, a Palestinian in Israel, a Mayan Indian in the streets of San Cristobal,… a Jew in Germany, a Gypsy in Poland, a Mohawk in Quebec, a pacifist in Bosnia, a single woman on the Metro at 10pm, a peasant without land, a gang member in the slums, an unemployed worker, an unhappy student and, of course, a Zapatista in the mountains» (Marcos, 1997).

All the different causes and struggles across the world coincide in their attack against the capitalist system: «These struggles do not link horizontally, but each one leaps vertically, directly to the virtual center of Empire» (Hardt and Negri, 2000: 58). Everyone is part of the multitude. In the same way everyone can be Anonymous:

> «How do I recognize other Anonymous?
>
> We come from all places of society: We are students, workers, clerks, unemployed; We are young or old, we wear smart clothes or rugs, we are hedonists, ascetics, joy riders or activists. We come from all races, countries and ethnicities. We are many.
>
> We are your neighbours, your co-workers, your hairdressers, your bus drivers and your network administrators. We are the guy on the street with the suitcase and the girl in the bar you are trying to chat up. We are anonymous. Many of us like to wear Guy Fawkes masks on demonstrations. Some of us even show them in their profile pictures in social networks. That helps to recognize each other».
>
> (Pastebin, 2013)

There is a strong cross-fertilization between political theory, social movements' practice and hacktivism. It is not by coincidence that the foreword of the anti-globalization movement book «Another World is Possible. Popular Alternatives to Globalization at the World Social Forum» (2004) is written by Hardt and Negri. This connection is not surprising and in fact reflects a particular vision of the role of political theory which is not so much an accurate description of the world but more a program, a manifesto for action. As Paul Patton claims in his article on Foucault and Deleuze, both of whom are widely quoted in «Empire»: «They reject the idea that there is a single 'totalising' relation between theory and practice in favour of a more local and fragmentary conception. Theory is neither the expression nor the translation of practice, but is itself a local and regional practice that operates as a series of relays from one practice to another, while practices are relays from one theoretical point to the next» (Patton, 2010: 86).

If we accept that theory and practice constantly inform and transform each other, the way to criticize and possibly improve a theory is through observing to what it leads in practice. This is precisely the goal of my paper. If Anonymous as a collective are the expression of an anarcho-communist theory/vision of the world, observing what they do and how they do it is essential to assessing this particular theory. My empirical analysis of the involvement of Anonymous in the anti-government protests has firstly the aim to assess anarcho-political theory on its own grounds, i.e. to explore whether Anonymous are in fact are open, inclusive and anti-capitalist, and second, to explore what is the political potential of such an organization in general compared to more institutionalized forms of political participation.

3. METHODOLOGY: «THE SILENCE OF THE LAMBS»

In order to analyze the involvement of Anonymous Bulgaria in the anti-government protests from June 2013, I performed content analysis of the two most popular Facebook pages of Anonymous Bulgaria from the beginning of the protests on the 14th of June until the 30th of June. In addition, I did a series of semi-structured in-depth interviews and frequented chat rooms of the group. I refer to the «Silence of the Lambs» in the title of this section not because the process of research resembled a horror film but because of an especially surreal conversation I had in one of the IRC chat rooms. The interview included myself under the pseudonym «pipi» and 7 respondents, who played a joke on me and changed their nicks to variations of the name «silentlamb»: silentlamb, stilenlamb, siletlamb, silenlamb, Silentlamb, stilenlabm. During the conversation one of them explicitly addressed the other telling him/her: «[17:08] <stilenlamb> Silentlamb, never give an interview!» In addition, one of the 7 people I was talking to turned out to be a bot. It is one of the rules of Anonymous never to give interviews which made my task especially difficult. What is more, as some of the activities of the collective could

be considered as cyber crime, I had to deal with constant suspicions that I was a police agent or a paid journalist.

In an attempt to establish initial contact, I posted on the largest forum of Anonymous Bulgaria a message about my project and promised to enter the two chats of Anonymous always with the same pseudonym «pipi» so that people knew that I was observing their conversation. The message on the forum provoked endless jokes and a wave of suspicion, one of the ironic responses I got being: «Hello, I am from the Cyber Crime Unit of the police and I work on getting a promotion by writing on Anonymous. Could you please answer some of my questions.....haahahahahah... :d :d :d :d :d» (Anonbg, 2013). My subsequent chat conversations made me painfully aware of the question of trust, with one of my respondents constantly checking random facts I told him in Google, repeating «I think you are lying to me» and refusing to answer some questions with the argument «you are going too far».

Due to the complex status of the actions of Anonymous, always on the border between legality and illegality, I was especially concerned about ethics issues. I decided to follow Stefania's Milan approach to adopt the hacker principles of «do not harm» and «leave no damage» as points of reference (Milan, 2012, 182). All interviewees used pseudonyms and encrypted connection. I didn't ask them about their real names so that I wouldn't be able to reveal them if asked by the police. I was also especially careful in terms of data storage and protected the interview data by keeping the files on a separate laptop without access to the Internet (Eynon et al., 2008, 28). With regard to the material from the public Facebook pages, I treat it as publicly available content and quote the authors of particular comments without asking for specific consent. In general, I adopted an approach to research ethics which is attentive to different contexts and their particular requirements instead of postulating in advance an overarching rule (Markham and Buchanan, 2012).

4. ANONYMOUS IN TIMES OF PROTEST

4.1. United as One, Divided by Zero

On the basis of the data collected, in the following paragraphs I will address the three sub-questions formulated in the beginning of this paper. First of all, who are Anonymous Bulgaria and what is their internal structure? There is active work involved in the process of group formation that includes the process of self-definition and differentiation from enemies (Latour, 2005, 34). It has to be clear that there is no single organization Anonymous Bulgaria. Instead, there are multiple loosely connected factions, each of which has its own Facebook page connected to a web site/forum, and two of them have their own IRC chats. In fact, the question «Who are Anonymous Bulgaria?» is relevant not only for me but for social actors as well. Some of the people in the two

chats I frequented were even less informed than I was, which made me question the border between observation and participation, externality and internality with regard to Anonymous. Many users join the channels where future operations are discussed out of curiosity and actively try to understand what the group does. As one user told me when I asked him about Anonymous: «I don't know either. I'm just hanging around trying to make sense». In addition, many people approach Anonymous for help with quite extravagant problems. Among the most typical examples are teenagers who want to have the Facebook profiles of their girlfriends hacked:

[01:54:27] Pafnuty Chebyshev: We tried to work responding to complaints by ordinary people
[01:54:44] Unfortunately people in Bulgaria are still in the stone age
[01:54:49] the only ones who approached us were the 12-13 year-olds with their stupid requests.

Often people are attracted by the media image of Anonymous and want to join them without having the necessary skills:

[02:25:22] Pafnuty Chebyshev: soon after the first attacks the first fans and try-hard-s appeared
[02:25:50] pipi: what does being a fan consist in? and trying-hard?
[02:26:28] Pafnuty Chebyshev: It consists in trying to participate in something the risks of which you cannot understand
[02:26:35] and in the lack of any programming skills

One of the factions of Anonymous has lost many members precisely because of the flow of new people in, the so called 'newfags':

[17:39] <Ch0v3ch3t0> Many people left us because of the newfags
[17:40] suddenly someone comes who doesn't know what Anon is
[17:40] and starts giving orders
[17:40] and you get fed up with all this and leave
[17:40] and others just lost any hope that something can change

But if 'newfags' don't know what Anon is, do more experienced users know? The answers they gave to my question were vague at best:

[17:04] <silentlamb> you can't say 'you're not anon!'
[17:05] 'Anonymous' and the 'Idea' are just metaphors meaning different things for different people
[17:05] <pipi> but if one word means everything, it actually doesn't mean anything
[17:05] <silentlamb> hmm
[17:05] <stilenlamb> Anonymous is just a word
[17:06] <silentlamb> they say that we are called 'Anonymous' because of the nicks in 4chan

This chat excerpt clearly shows the difficulty to define Anonymous, to state what it means to be part of the group. My question for definition is displaced and addressed as a question of genealogy or even etymology, tracing the origins of the group name.

However, the absence of clarity is not due to some confusion. The inability to strictly define Anonymous is inscribed in the very ideology of the collective. It is an

essential part of who they are. The instruction on how to recognize other Anonmous, quoted in the theoretical review section is repeated almost literally by one of my respondents in the chat room:

> [17:21] <stilenlamb> Among us there are journalists, writers, students, engineers, cleaners, butchers
> [17:21] We are not just hackers. We are your neighbour, your classmate...
> [17:21] Anyone can be Anon...

Yet, there are limits to the openness of the group. Anyone who claims to be a leader of the movement cannot be Anonymous, neither can be traditional politicians or political parties, often accused in my interviews of infiltrating the «authentic» pages of the group. On the wikianonbg.com web site there is even a wall of shame with the names of people who have tried to «hijack» the cause. Or to put it simply, everyone can be Anonymous but some are more Anonymous than others.

> [17:48] <Ch0v3ch3t0> Everyone who knows the idea knows that no one from Anon
> [17:48] would use the idea to support a political party

The attitude towards politics is one of the main criteria for differentiation between the different factions of the group. Pafnuty Chebishef has left Anonymous because according to him people have betrayed the idea and have started to get involved in political causes, to plan to participate in elections, etc. According to pafkata86, one of the factions of Anonymous Bulgaria fights against government parties, while the other attacks private organizations such as monopolists in electricity supply, water supply, etc. In a nutshell, some members of Anonymous are against the politicization of the cause in general, while those who claim that Anonymous should have a say in politics differ in their very definition of politics and the causes they support.

Another source for internal differentiation within Anonymous Bulgaria is technical expertise. At the time I was conducting the interviews the programmers' core of one of the factions had left, leaving the young ones to cope alone. Know-how is extremely important for Anonymous and is transmitted through personal contact online and with the help of tutorials. Technology is a main uniting force for the group and the reason many people join in. Thus, Pafnuty Chebyshev started his involvement with Anonymous by finding the unfinished forum anonbg.info. After a short contact with the system administrator he became the global moderator of the community. The forum was left by a previous Anonymous group which had disbanded more than a year ago because of differences in political ideology. Once Pafnuty resurrected the forum, 2 more people joined and a new community was formed. Their main activity in the beginning was the exchange of technical knowledge «in the name of the greater good».

But forums and web pages are used not just for recruitment and consolidation. My observations during the protests showed that Facebook pages can be stolen from within by group members with different vision for the future. What is more, one of the web

pages I was observing (wikianonbg.com) was taken down while I was doing my research. Another subversive practice is to copy and paste messages from one chat room to the other in order to make fun of particular users. Channels for communication can have a deeply political use and allow strategic displacement of discussions and hijacking of symbolic capital.

To sum up, the very question 'Who are Anonymous Bulgaria?' is a political question which is still to be decided. The faction that manages to create the most durable association between people, online platforms, software and hardware will probably impose its vision (Callon and Latour, 1981). For the time being, there is no unity but mainly division, no group, but group formation. Anonymous Bulgaria are in a state of productive uncertainty in which they have to choose their future.

4.2. I like to lumpen lumpen

The second sub-question I am going to address is: in what ways did Anonymous engage in social critique in the period 14th-30th of June? In answering this question I will count on the content analysis of the posts and comments on the two most popular Facebook pages of Anonymous Bulgaria. There is clear difference in the main focus of the two pages.

Anonymous Bulgaria (3,431 likes) was engaged with causes such as data privacy (with various posts about Edward Snowden and surveillance in the US) and international solidarity. One could read on their Facebook page posts in English such as the following:

> #OccupyBulgaria #OccupyGezi #ChangeBrazil - WE ARE ONE
>
> It's not over. #Revolution @AnonOpsMob: Army of people getting ready to retake #Taksim Square again http://t.co/uJhRZtdBQ9
> #Anonymous #OccupyGezi
> Rise up!

And also the motivational:

> United as one divided by zero!
> #AnonymousBulgaria
> #AnonymousTurkey
> #AnonymousBrazil

The team of REVOLUTION announces that Turkish users show a serious interest in the protests in Bulgaria. They actively share and comment on our pictures, one can clearly see SOLIDARITY!

(Anonymous Bulgaria, 2013)

On the contrary, the more popular group ANONYMOUS BULGARIA (12, 822 likes) focused on current political events in Bulgaria. The content analysis revealed that

the most prominent themes were: the anti-government protest; the proposed changes in the educational programme leaving out important poems by the 19th century national poet and revolutionary Hristo Botev; the exploitation of gold mines by foreign companies; the forbidden relations between political enemies, media owners and mafia bosses; the fierce opposition to the so called ‘Harta 2013’ [Chart 2013] that contained ideas for political reform suggested by Bulgarian intellectuals.

In the period observed there were also two operations of Anonymous. The first of them was reported on the Facebook page of Anonymous Bulgaria. It consisted in defacing the website of the Youth Organization of the ruling Socialist Party. The reason for the anger of Anonymous was a statement made by a socialist politician, who claimed that the current protests are caused by ‘the Internet lumpenproletariat’. The phrase became an instant hit. People started going to the protests with signs «I am an Internet lumpen», contributing to the Facebook hashtag #internetlumpeni, and even jokingly performing in front of the National Assembly a song with the lyrics: «I like to lumpen lumpen»: <http://www.youtube.com/watch?v=fcrjNkote5s>. The second operation was published on both Facebook pages, but the massive campaign around it was associated exclusively with the ANONYMOUS BULGARIA page. The hacktivist group defaced the website of Harta 2013, claiming that NGOs and intellectuals are trying to become leaders of an essentially horizontal citizen protest and to «trick» common people. Both operations and the content of both Facebook pages are indicative of the deep mistrust in politics in any institutionalized form.

Probably the best summary of social critique during the protest is afforded by the following image (fig. 2):

Fig. 2. Photo from the protests. Source: ANONYMOUS BULGARIA, 2013.

The black sign in the foreground reads: «Corruption entered in parliament again and chose its own government», the black sign in the background reads «Against the invasion of Turkish masses» and the white sign reads: «Change of the system, New Constitution». The picture is published on the ANONYMOUS BULGARIA page with the question: «Do you think that the flag of the European, pardon Jewish, Union should be there?»» with comments such as «In Bulgaria - only what is Bulgarian» and «Burn it!» (ANONYMOUS BULGARIA, 2013).

I analyze this image and its context in light of Boltanski's theory of social critique. The accusations of corruption and the unmasking of corrupt politicians seem a good example of what Boltanski calls 'tests of reality'. The critique is directed against the spokespersons of the institutions but not against the institutions themselves. The «Change of the System: New Constitution» slogan however points to a more radical critique which insists on a total social change. One of the key problems in the June 2013 protests in Bulgaria was that social critique was directed against everyone and everything which led to an impasse: an all-pervading sense of apathy and negativism. The logical counterpart of such insecurity was the return to romanticized forms of bonding and stability. Conspiracy theories went hand in hand with nationalism. Critique as performed by Anonymous was at the same time anti-institutional («Fuck the system!») and conservative («Bulgaria for the Bulgarians!»).

4.3. Decision making on the ground: searching for alternatives

The third sub-question that I tried to answer by analyzing the available data relates to the alternatives to the current social order proposed by Anonymous Bulgaria. If the position of the collective has to be summed up in two words, they have to be: direct democracy. The actions against both party-affiliated politicians and civil society intellectuals showed a clear suspicion of political representation as such. The alternative offered is participation by everyone facilitated by technology:

> ANONYMOUS BULGARIA direct democracy is a form of political organization of the society, in which the main decisions are accepted and implemented directly by citizens - notice that we talk precisely about citizens, you are included there, as well as your neighbour and your grandmother from her godforsaken village. Direct Democracy is the unmediated way to take decisions in a society. This means from us for us, without leaders, representatives, instructors, etc. Of course it can't happen immediately. All public assemblies can be connected and each one can have a representative. This means that the assembly can be in your village/neighbourhood/city and everyone can participate. Bulgarian citizens can participate virtually over the Internet (ANONYMOUS BULGARIA, 2013).

The principles that Anonymous envisage for reforms are the very principles that structure their group. Complete openness, inclusiveness and direct participation seem to replace the need for any institutionalized form of politics. However, disintermediation is never that innocent, and presupposes the creation of new intermediaries (Gra-

ham, 2008). There are several problems with replacing political mechanisms of representation with technological mediation. First of all, a major issue is access to technology. Not everyone can participate and technology creates new inequalities (Graham and Haarstad, 2011). For some, this is an advantage:

> Elza In the social networks one cannot find the darker-skinned electors of the current parties [the comment refers to the gypsies] (ANONYMOUS BULGARIA, 2013).

But if technology can be used to exclude people, this leads to an internal contradiction in the very ideology of openness and inclusiveness.

In addition, ANONYMOUS BULGARIA defended the idea of public assemblies in which people sit on the ground, because «nothing can happen under the table». But how often would people find time to sit on the ground and collaborate? How much time are they prepared to sacrifice? To illustrate, Anonymous encouraged discussions on their Facebook page for possible changes in the political system. In response several users posted long lists with ideas for political change. The user Georgi Karadachki in a comment from the 16th of June proposed to publish all dossiers of former state security agents, to forbid them participation «in the political, economic and social life in the country», to introduce electronic voting, to challenge the monopoly of the National Health Insurance Fund, etc. (ANONYMOUS BULGARIA, 2013). Some of these ideas seem a bit extreme –preventing people from any participation in social life because of past mistakes, or making all policemen pass a lie detection test– but the problem is not so much in the content of the suggestions as in their rather piecemeal character.

In addition, ANONYMOUS BULGARIA recognized the need to discuss initial suggestions and develop a more coherent system. That is why they published a special note (Anonymous Note, 2013), which was supposed to be constantly expanded and changed through citizen proposals. But there was a serious lack of interest and user participation. Only 10 people commented on the note. And it is doubtful whether the opinions of 10 people were enough to propose substantial changes that could be perceived as legitimate.

To sum up, the increase in participation and openness in the alternatives to current forms of democracy proposed by Anonymous should be balanced against the dangers of technological exclusion, piecemeal solutions and under-participation.

5. DISCUSSION AND CONCLUSION: THE WILL TO BE AGAINST

Hardt and Negri have proposed a vision of international inclusive collaborative networks of resistance. Networks unified by recognizing and constructing what we have in common: «It is not really a matter of fixing a point of unity or, worse yet, identity, but simply finding what is common in our differences and expanding that commonality

while our differences proliferate» (Hardt and Negri, 2003, 17). It is this same vision of collaborative international resistance that has informed the ideology of the Anonymous collective. My empirical observations, however, point to the fact that Anonymous Bulgaria, as they operate on the ground, have concerns which are much more local, related to issues of the nation and nationhood. Indeed one of the factions of the group (Anonymous Bulgaria) demonstrates international solidarity and interest in information and human rights in general. But the faction which is much more popular (ANONYMOUS BULGARIA) is the one that addresses very narrow locally-specific political issues such as the school program, a project by local intellectuals or the biographies of particular politicians. In addition, fighting against capitalism is not among the priorities of the Bulgarian Anonymous. On the contrary, they fight against Mafia and corruption, against the shape that institutions have taken in Bulgaria here and now. Thus, while transnational organization and diffusion of the brand Anonymous is undoubtedly important, the importance of the nation state as a locus of resistance not only has not diminished, but on the contrary –it has increased.

When it comes to the internal organization of the group, it is inevitable to notice that instead of complete inclusiveness and convergence of different types of struggles against a common goal, what is observed is fragmentation and dissent on the basis of both political differences and differences in the levels of technical skill. Vertical struggles do not «magically» coincide and hit «the virtual center» of Empire. On the contrary, as Laclau convincingly argues, there is a painful process of political articulation and horizontal coordination of struggles that is inescapably political and is related to processes of exclusion, of defining «us» and «them» (Laclau, 2004, 28). And this process takes place even in a movement that explicitly states that «everyone is Anonymous» –it takes place against its very own ideology.

What is more, the atmosphere of all pervasive suspicion and «fuck the system» attitude does not allow Anonymous to formulate a targeted critique and instead leads to a dispersed, conspiracy-theory-driven series of actions with little political traction. The mistrust of any form of institutions and constituted power is a defining feature not only of Anonymous as an actually operating hacktivist formation but also of the theory that has inspired them. To illustrate, Paul Patton identifies as a serious reason for dissent between Foucault and Deleuze the latter's state phobia. According to Foucault not all states are the same and not all institutions are bad: «Foucault objects to the essentialism of the state phobic conception that it licenses the 'interchangeability of analyses and the loss of specificity'» (Patton, 2010: 93).

The will to be against does not spontaneously lead to social change. A positive vision of what we are fighting for must be provided. The multitude is powerful but this power can be used for bad. As Slavoj Zizek reminds us: «in Spinoza, the concept of multitude qua crowd is fundamentally ambiguous: multitude is resistance to the imposing One, but, at the same time, it designates what we call 'mob', a wild, irrational explosion

of violence» (Zizek, 2007). It seems that Hardt and Negri neglect this «bad» side of the multitude. What if the multitude desires something utterly destructive? Is nationalist violence also part of the «productive force of the multitude»?

And again, following Zizek, what will happen if the multitude takes over? (Zizek, 2006). Is it really possible to go without constituted power? Or representative democracy will be replaced with new forms of charismatic informal leadership (Gerbaudo, 2012)? The alternatives to the current political system proposed by Anonymous are all procedural. They offer ways of avoiding the traditional system of representation. But as Della Porta and Diani argue, the practical functioning of these alternative organizational structures is much less than perfect: «Unstructured assemblies tend to be dominated by small minorities that often strategically exploit the weaknesses of direct democracy with open manipulation; 'speech' resources are far from equally distributed; the most committed, or better organized, control the floor; solidarity links tend to exclude newcomers. Consensual models developed to contrast the 'tyranny' of organized minorities have their own problems, mainly bound up with extremely long (and sometimes 'blocked') decision processes» (Della Porta and Diani, 2006, 244).

To sum up, the «artistic critique» of capitalism provided on a theoretical level by Hardt and Negri and embedded in the organizational structure of the hacktivist collective Anonymous cannot so far provide a viable alternative of the current political system. The state phobia and the mistrust of institutions lead to too quick dismissal of the role of state and questions of redistributive social justice. The will to be against is not enough. Anonymous are raising a crucial question about politics as it is. But they are not the answer.

6. BIBLIOGRAPHY

Anon2k13 (2013): So You Want to Join Anonymous? <http://pastebin.com/SqhHjuGu> [4 March, 2014].

Anonbg (2013): Forum of Anonymous Bulgaria <http://anonbg.info/> [18 July 2013].

Anonymous Bulgaria (2013): <https://www.Facebook.com/anon.bg?fref=ts> [10 February 2012].

ANONYMOUS BULGARIA (2013): <https://www.Facebook.com/AnonyBulgaria?fref=ts> [10 February 2014].

Anonymous Note (2013): <https://www.facebook.com/notes/anonymous-bulgaria/%D0%B1%D0%B5%D0%BB%D0%B5%D0%B6%D0%BA%D0%B0/469601176461438> [10 February 2014].

ANON OPS (2010): A Press Release, ANONNEWS <http://anonnews.org/?p=press&a=item&i=31> [4 March, 2014].

Boltanski, L. (2011): On Critique: A Sociology of Emancipation. London: Polity Press.

Boltanski, L. and E. Chiapello (2005): The New Spirit of Capitalism. London and New York: Verso.

Callon, M. and B. Latour (1981): Unscrewing the Big Leviathan: how actors macrostructure reality and how sociologists help them to do so. In: K. D. Knorr-Cetina and A. V. Cicourel (eds.) Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies. Boston, Massachusetts: Routledge and Kegan&Paul, 277-303.

Coleman, G. (2012): Our Weirdness is Free. Triple Canopy. <http://canopycanopycanopy.com/15/our_weirdness_is_free> [2 of March, 2014].

Coleman, G. (2011): From the Lulz to Collective Action. <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action> [3 March, 2014].

Della Porta, D. and M. Diani (2006): Social Movements. An Introduction. Second Edition. Oxford: Blackwell Publishing.

Eynon, R. et al (2008): The Ethics of Internet Research. The Sage Handbook of Online Research Methods (Fielding, N., Lee, R. and Grant, B., eds.). London: Sage.

Free Software Foundation (2013): *What is Free Software?* <http://www.gnu.org/philosophy/free-sw.html > [17 February 2014].

Gerbaudo, P. (2012): Tweets and the Streets. Social Media and Contemporary Activism. London: Pluto Press.

Graham, M. & Haarstad, H. (2011): Transparency and Development: Ethical Consumption Through Web 2.0 And the Internet Of Things. Information Technologies and International Development. 7(1). 1-18.

Graham, M. (2008): Warped Geographies of Development: The Internet and Theories of Economic Development. In: Geography Compass 2 (3): 771-789.

Hardt, M. and A. Negri (2005): Multitude: War and Democracy in the Age of Empire. New York: Penguin Books.

Hardt, M. and A. Negri (2003): Foreword. Another World is Possible. Popular alternatives to globalization and the Social World Forum (Fisher, W. and T. Ponniah, eds.). Nova Scotia: Fernwood Publishing.

Hardt, M. and A. Negri (2000): Empire. Cambridge and London: Harvard University Press.

Jordon, T. and P. Taylor (2004): Hacktivism and Cyberwars: Rebels with a Cause. London and New York: Routledge.

Kelly, B. (2012): Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and should influence cybersecurity reform. *Boston University Law Review, 92 (5)*: 1663–1710.

Laclau, E. (2004): Can Immanence Explain Social Struggles? *Empire's New Clothes* (eds. P. Passavant and J. Dean). New York and London: Routledge, 21-30.

Latour, B. (2005): Reassembling the Social. An Introduction to Actor-Network Theory. Oxford: Oxford University Press

Levy, S. (1984): Hackers: Heroes of the Computer Revolution. New York: Anchor Press/Doubleday.

Marcos (1997): Marcos is Gay. < https://www.greenleft.org.au/node/16118 > [4 of March, 2014].

Markham, A. and E. Buchanan (2012): Ethical Decision-Making and Internet Research: Version 2.0. Recommendations from the AoIR Ethics Working Committee. <http://aoir.org/reports/ethics2.pdf> [13.03.2013].

Milan, S. (2012): The Guardians of the Internet? Politics and Ethics of Cyberactivists (and of their Observers). Inter-Asia Roundtable 2012: Methodological and Conceptual Issues in Cyber Activism Research, 167-191.

Negri, A. (2004): Subversive Spinoza. (Un)contemporary variations. Manchester and New York: Manchester University Press.

Passavant, P. (2004a): Postmodern Republicanism. *Empire's New Clothes* (eds. P. Passavant and J. Dean). New York and London: Routledge.

Passavant, P. (2004b): From Empire's Law to the Multitude's Rights: Law, Representation, Revolution. *Empire's New Clothes* (eds. P. Passavant and J. Dean). New York and London: Routledge.

Patton, P. (2010): Activism, Philosophy and Actuality in Deleuze and Foucault. Deleuze Studies, Volume 4, 84-103.

Stallman, R. (2002): *Free Software, Free Society: Selected Essays*. Boston: GNU Press.

Zizek, S. (2007): *Spinoza, Kant, Hegel and...Badiou!* <http://www.lacan.com/zizphilosophy1.htm> [19.01.2014].

Zizek, Slavoj (2006): *Blows against the Empire?* <http://www.lacan.com/zizblow.htm> [19.01.2014].

LA DESREPRESENTACIÓN POLÍTICA. POTENCIALIDAD DE INTERNET EN EL PROCESO LEGISLATIVO

Francisco Jurado Gilabert
Jurista. Investigador en el Laboratorio de Ideas y Prácticas Políticas de la Universidad Pablo de Olavide. Doctorando en Filosofía del Derecho y Política en el IGOP, Universidad Autónoma de Barcelona

RESUMEN: El modelo de representación parlamentaria de las democracias contemporáneas empieza a envejecer. La participación política de la sociedad, limitada en gran medida al sufragio, se antoja insuficiente y se extiende la percepción de que los cargos electos no cumplen su función de representar. En este contexto, el desarrollo de las tecnologías de la comunicación ofrece un nuevo campo de posibilidades de acción política desintermediada que, a su vez, pueden corregir las patologías del modelo actual: corrupción, acumulación y abuso de poder o el distanciamiento entre las instituciones y la gente.

En concreto, en la tarea de legislar y aprobar lo legislado, emergen iniciativas que promueven la elaboración abierta y colaborativa de los textos legales, así como la implementación de sistemas de votación directa de los mismos. En definitiva, una nueva ola de propuestas que persiguen que la sociedad se reapropie de una política institucional que cada vez resulta más lejana y más ajena.

PALABRAS CLAVE: Desrepresentación, tecnopolítica, voto telemático, proceso legislativo, eDemocracy.

1. INTRODUCCIÓN

1.1. Contexto

En Febrero de 2013, Metroscopia publicaba una encuesta[1] sobre la percepción que los ciudadanos tenían del papel y la labor del Congreso y de sus diputados en España. Los resultados arrojaban que el 74% de los encuestados consideraban que «el Congreso no representa a la mayoría de los españoles», y hasta un 80% aseguraban «no sentirse personalmente representados». El detalle de la encuesta muestra, además, que esa percepción es de largo abrumadora también entre los electores de los dos partidos mayoritarios.

Los resultados de esta encuesta tienen una relación directa con otros datos. En primer lugar, con los sondeos periódicos que realiza el Centro de Investigaciones Socioló-

1 FERRÁNDIZ, J. P. (2013). *No nos representan.* Blog de Metroscopia en El País. Recuperado el 30 de enero de 2014 desde http://blogs.elpais.com/metroscopia/2013/02/no-nos-representan.html

gicas (CIS) que, en su último informe (Diciembre de 2013)[2], indica que los principales problemas, a ojos de los ciudadanos, son «el paro», «la corrupción y el fraude», «los problemas de índole económica» y «los políticos, los partidos y la política», en ese mismo orden, pudiendo considerarse éste último como un problema aglutinador del resto, pues de la acción y dirección política se desprenden en gran medida los demás.

Por otra parte, al leer o escuchar el *meme* «no nos representan», es inevitable evocar el grito multitudinario que se viralizó y replicó desde los ámbitos del Movimiento 15M. No quiere decir esto que no fuese preexistente, que no existiese antes esa sensación, sino que, a raíz de las manifestaciones, de las acampadas y de la fuerza de la autocomunicación[3] en red, su verbalización y reproducción se hizo masiva creando, a modo de eslogan performativo, una realidad social.

Ese pensamiento común –no nos representan– contrasta con el artículo 66.1 de la Constitución Española, que establece que «Las Cortes Generales representan al pueblo español y están formadas por el Congreso de los Diputados y el Senado», dando lugar a una especie de disonancia cognitiva entre lo que dictamina el ordenamiento jurídico y la opinión pública mayoritaria acerca del papel y la labor de uno de los poderes del Estado. Esta incongruencia, en un Estado Democrático y de Derecho, afecta directamente al encaje, entre sí, de elementos y principios fundamentales como el «imperio de la Ley», la «voluntad soberana popular» y el «interés general»[4].

Cabe y es pertinente cuestionarse si el modelo dispuesto en el ordenamiento vigente, en lo relativo a la labor de los diputados, a los mecanismos de configuración y funcionamiento de las cámaras, al proceso legislativo o, en su conjunto, es eficaz a la hora de adecuar la toma de decisiones políticas a la *voluntad soberana popular* (1.2 CE).

Subyace a estas cuestiones el debate general sobre la representación política en las democracias parlamentarias contemporáneas, en cuanto a sus límites, sus fallas y su combinación con otros modos de acción y participación en la propuesta y toma de decisiones.

1.2. Marco teórico y estructura

El presente trabajo parte de un análisis de los sistemas de representación parlamentaria contemporáneos, acerca de los cuáles se realiza un diagnóstico que pueda apuntar algunas razones de las fallas en su funcionamiento, siempre desde la óptica de un diseño

2 Centro de Investigaciones Sociológicas. *Percepción de los principales problemas de España.* Barómetro de Diciembre de 2013. Recuperado el 30 de enero de 2014 desde http://www.cis.es/cis/export/sites/default/-Archivos/Indicadores/documentos_html/TresProblemas.html

3 En el sentido de CASTELLS.

4 En el preámbulo de la Constitución Española se establece el propósito de «consolidar un Estado de Derecho que asegure el imperio de la Ley como expresión de la voluntad popular».

–ingeniería institucional (Przeworski, 1998)– orientado a la toma de decisiones basada en el interés general[5]. Esto no quiere decir que sea el único teórico sobre la función de gobierno, pero mi decantación se funda, primero, en los límites fijados a la extensión del trabajo y, entroncado con estos, en lo pragmático de centrarse en la visión dominante, al menos, en los fundamentos jurídicos de las constituciones vigentes.

Dentro de este marco, centro el análisis en la figura de la representación política, como mecanismo habilitador de la acción de gobierno de «unos pocos» en nombre y por cuenta de una generalidad que lo es es un doble sentido: institucional en relación a la Administración y sus órganos, y colectiva al fundarse sobre un grupo humano que la compone (alrededor del estatus de ciudadanía), la sostiene (mediante un sistema tributario) y es, a su vez, sujeto y destinatario de la acción de gobierno. La aproximación a la representación se acomete fundamentalmente desde el trabajo de Pitkin y otros autores (Cotta, Ferrajoli, Sartori y otros).

El objetivo es observar como la posición de los representantes, en los sistemas actuales de representación, los conforma en un núcleo de poder difícilmente fiscalizable, con lo que se quiebra uno de los principios fundamentales de la acción de la representación, la *accountability* (Pitkin, 1967; Przeworski, 1998; Sartori 1999; y otros).

Como mecanismo corrector de esta falla en la institución de la representación se propone la capacidad de *desrepresentarse* a través de dos fases del proceso legislativo, la proposición y la votación de las normas. El motivo de la descripción como actos de *desrepresentación*, en lugar de como ejercicios de democracia directa, es la toma, como punto de partida, de un estadio de representación legal/forzosa, sobre la que se regularían estos ejercicios de recuperación de una soberanía popular (1.2CE) que, *de iure et de facto*, viene depositada en los representantes. Entonces, estaríamos hablando de mecanismos tradicionales de democracia directa ejercidos bajo la forma de un «*recall*» (o revocatoria), pero distinguiéndose de este concepto clásico en la temporalidad, ya que la *desrepresentación* actuaría en tiempo real y sin necesidad de una convocatoria y procedimiento especiales.

Es necesario, por tanto, aproximar la naturaleza jurídica de la representación política, ubicarla dentro de los diferentes tipos de representación regulados en el ordenamiento y, entonces, comprobar cómo se puede realizar el encaje jurídico de la *desrepresentación*, como propuesta de institución *ex novo.*

En ese análisis de los componentes que han hecho de la representación política una institución forzosa, inamovible, invariable e incuestionable, se observa que gran parte de

5 Siendo un concepto amplio y de cierta abstracción, lo circunscribiré en el sentido que se le da en el artícuo 103 de la Constitución española, que recoge, en gran medida, la orientación dada en las democracias contemporáneas al interés público o interés General, y que se puede consultar en http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=103&tipo=2

las motivaciones estaban basadas en límites espacio-temporales que aconsejaban, de cara a la gobernabilidad, la acción a través de representante. Hoy día, sin embargo, las tecnologías de la comunicación permiten una participación masiva y de coste reducido (en comparación, por ejemplo, a las votaciones con urnas), en procesos como la elaboración colectiva de textos legales o en su votación directa. Es por ello que Internet transforma las condiciones materiales del ejercicio práctico de la política, remueve los límites físicos preexisstentes y plantea, de manera potencial, un nuevo horizonte de participación política desintermediada.

2. DIAGNÓSTICO: CRISIS DE LA REPRESENTACIÓN POLÍTICA

2.1. Desplazamiento del proceso crítico

Un proceso crítico, en la literatura empresarial, es aquél, significativo y fundamental, vinculado a la actividad y al servicio que presta una organización. Al realizar esta analogía en el campo de la política institucional, pretendo describir como proceso crítico a aquél del que se desprenden todos los demás procesos y direcciones políticas de un gobierno; al proceso que determina, sistemáticamente, la composición y el funcionamiento de los órganos e instituciones de la Administración.

Según el esquema triádico de la división de poderes, de sus potestades y su composición, es el legislativo, materializado en sus cámaras, el proceso que condiciona, a través de su funcionamiento, el de los demás. Del legislativo salen las normas que rigen al resto y, en gran medida su composición.

Sin embargo, hay que dar un paso más para ver cómo se componen las cámaras legislativas, de dónde resultan, si queremos comprender las dinámicas de poder reales que, a la postre, explican las disonancias antes citadas entre esa voluntad popular y la política institucional. Esto nos lleva inequívocamente al proceso electoral, esa cita trascendental que acaece cada 4 años y que determina el juego de mayorías y minorías que legislarán y gobernarán durante ese amplio periodo de tiempo.

Los comicios electorales son un «juego de suma cero», un modelo particular en Teoría de Juegos no cooperativos, donde la ganancia o pérdida de un participante se equilibra con las ganancias o pérdidas del resto de participantes. Al plantearse las elecciones en estos términos, se impone como estrategia dominante la competición, agravada por el comportamiento estratégico de las élites de los partidos que, en función de la legislación electoral, se podría calificar como irracional[6].

6 En este sentido, GÜNTHER, R. (1989). Leyes electorales, sistemas de partidos y élites, *Reis: Revista Española de Investigaciones Sociológicas, nº* 47, pp. 73-106.

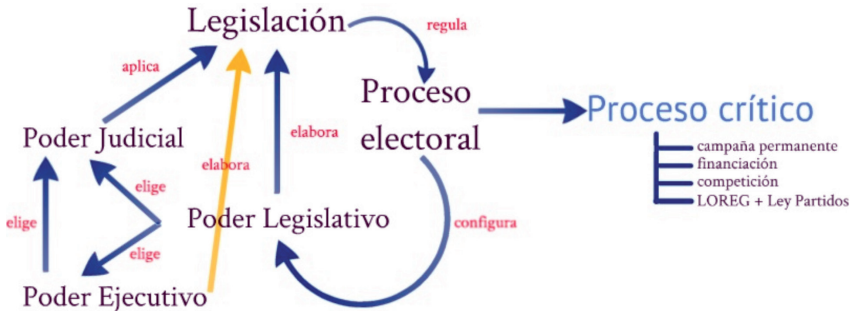


Ilustración 1: Desplazamiento del proceso crítico. Elaboración propia

Es en las elecciones donde se debe materializar uno de los elementos que componen el concepto de representación política, la «rendición de cuentas» (o *accountability)*[7], materialización que se produce, además, a través de otro de sus elementos, la posibilidad de destitución (*removability)*, transformada en cierto modo en «no reelección». Sin embargo, como apuntaba anteriormente con el caso de las élites de los partidos, el comportamiento electoral dista de ser una conducta puramente racional y, además, las listas electorales de la mayoría de los partidos (o de los más representados) están fuertemente condicionadas o directamente confeccionadas por sus propias direcciones, por lo que las posibilidades de realizarse tanto la *accountability* como la *removability* se ven fuertemente limitadas.

Al final, las relaciones entre los 3 poderes (o ámbitos del poder) del Estado quedan sujetas al proceso electoral, a la campaña permanente, a las posibilidades económicas de las que disponga un partido a la hora de competir con los demás (en comunicación, en presencia, en recursos) o a las barreras a la entrada que se levantan utilizando la propia legislación electoral (los avales a las nuevas formaciones, los métodos de escrutinio, etc.). Las elecciones se convierten en el verdadero *proceso crítico*.

2.2. Sobre la representación política y su naturaleza jurídica

Siguiendo la clasificación que hace LIFANTE VIDAL[8], apoyándose en otros autores, la *representación práctica*[9] puede constar de tres tipos:

7 SARTORI, G. (1999). En defensa de la representación política. *Claves de razón práctica*, nº 91, p. 4. y, sobre el trabajo de PITKIN, una reconstrucción de GARCÍA GUITIÁN, E., 2001. Crisis de la representación política: las exigencias de la política de la presencia. *Revista de Estudios Políticos*, nº 111, pp. 215-216

8 LIFANTE VIDAL, I., (2009). Sobre el concepto de representación. *DOXA, Cuadernos de Filosofía del Derecho*, 32. ISSN: 0214-8676 pp. 515-519

9 Consistente en *actuar por o en lugar de* (COTTA, 1983, p.1426), contra puesta a la idea de r*epresentación simbólica*, centrada más en *est*ar *por o en lugar de* (LIFANTE, 2009, p.512).

a) La representación individual, que se suele dar en el ámbito del Derecho Privado y que se suele denominar representación privada, donde el sujeto representado es uno (o considerado de manera individual).

   Dentro de este tipo de representación práctica, podemos, a su vez, diferenciar entre una representación voluntaria, que nace de la propia voluntad del representado, del apoderamiento que otorga al representante, y la representación forzosa o legal, que suele venir determinada por la ley o mediante sentencia judicial[10]. La diferencia fundamental entre ambas radica en la voluntad del representado, considerándose ésta como no existente, insuficiente o minusvalorada en los supuestos de representación legal/forzosa.

b) La representación institucional, donde lo representado es una construcción artificial (normalmente jurídica), a la que no se le pueden imputar acciones, siendo éstas realizadas por su(s) representante(s). En este caso no se representa a los individuos que hayan podido crear ese constructo, sino a la cosa misma, que no existe con anterioridad a la propia relación de representación[11].

c) Por último, la representación colectiva, donde el sujeto representado consiste en una pluralidad de personas, agrupadas en colectivo, que comparten intereses en tanto poseedoras de una característica común. En este sentido, no se pretende representar a cada uno de los individuos, sino un aspecto común a todos ellos.

La representación política no puede subsumirse en una sola de esas categorías, sino que comparte elementos de las tres. A primera vista, tiene mucho en común con la representación colectiva, siendo el estatus de ciudadano el elemento aglutinador de la comunidad a la que se representa. Pero también hay elementos de representación institucional, más ligados con la componente simbólica de la representación[12]. Por último, aunque parezca la más lejana, hay ciertas características de la representación individual

10 Salvo en el caso de la representación procesal que, aún considerándose legal, requiere de apoderamiento.

11 HOBBES (1980, p.135) identifica a la representación política como representación institucional, algo bastante discutible, precisamente porque eso significaría certificar que una comunidad de personas no preexiste a la organización política que deseen establecer en cada momento histórico. En nuestro caso, dado el reconocimiento constitucional del sujeto colectivo «pueblo español», no se puede afirmar que ese sujeto no sea preexistente a la propia Constitución, ni que le sea sustraída la capacidad para actuar políticamente, aunque en la actualidad se reduzca a poco más que las Iniciativas Legislativas Populares. Por último, podemos afirmar que en la relación que nace en la representación política, los actos que acomete el representante recaen no sólo sobre la construcción jurídica (Estado, Comunidad, Administración Local), sino también sobre los propios representados.

12 R4 en Pitkin, 1967.

que, a la postre, resultan fundamentales para comprender la posición de poder-dominación que surge de la relación de representación política, y que se desarrollarán después.

Como describe Przeworski, nos encontramos con una representación donde una de las partes se compone de una oligarquía (aristocracia en sentido aristotélico) que compite entre sí (Schumpeter, 1942; Dahl, 1971; Bobbio, 1989) por recibir el mandato de una comunidad a la que pretende representar y gobernar. Este diseño permite, en teoría, combinar la autoridad necesaria para mandar y determinadas precauciones, verticales (las elecciones) y horizontales (pesos y contrapesos entre los poderes) para impedir un ejercicio demasiado arbitrario de ese mandato, toda vez que el mandato imperativo está descartado, tanto por la legislación como por su imposibilidad material[13]. De este modo, la acción del representante cuenta con una gran dosis de discrecionalidad, operando la rendición de cuentas en dos direcciones: una, respecto de los electores, que sucede en ocasiones puntuales cada cierto tiempo, en las elecciones, y otra respecto al partido al que pertenece, siendo ésta más constante y determinante, habida cuenta de que, salvo en los procesos de primarias abiertas, la inclusión de un candidato en unas listas electorales depende en gran medida de su organización política, que cuenta, además, con otros mecanismos disciplinarios, como las sanciones, los expedientes y la expulsión.

A pesar de que existen corrientes como las de la teoría de la agencia, en la que los ciudadanos son vistos como principales y los representantes como agentes, esta relación sigue flaqueando en la misma pata: cómo fiscalizar la acción de agencia en tiempo real, cómo definir el mandato más concretamente que con nociones generales y marcos categoriales ideológicos, o de una manera más fiable que la que ofrecen los programas electorales, que no albergan ningún tipo de garantía de cumplimiento.

Nos encontramos, por tanto, ante un tipo de representación que contiene una indeterminación fundamental en su elemento teleológico, en la determinación del fin último de la labor del representante. Este contenido puede estar inspirado por principios generales del derecho y la Administración, como el Interés General (103CE) o beber de otras corrientes de corte más liberal, que reconstruyan ese interés púbico desde la protección y defensa de derechos individuales[14]. Sea como fuere, determinar si la orientación legislativa se adecua a la defensa de los intereses de los representados[15] (concebidos como una subjetividad colectiva o de manera individualizada) es harto complicado.

Por otra parte, si analizamos lo dispuesto en el Reglamento del Congreso, en relación con el Estatuto de los Diputados, no encontraremos referencia alguna al modo o a los principios inspiradores que deben informar y condicionar el ejercicio de su cargo. Muy por el contrario, este ejercicio se ve fuertemente condicionado por una norma no

13 *Cfr*. SARTORI, G. 1999, p.3

14 C*fr* C. Offe y U. Preuss, «Instituciones democráticas y recursos morales». Isegoría, nº 2, 1990.

15 R5 en Pitkin, 1967.

escrita, popularmente conocida como «disciplina de voto», que pretende unificar el criterio de los diputados pertenecientes e un mismo partido político[16].

El papel central que ocupan los partidos políticos en la determinación de la conducta de los cargos electos supera la vinculación de los mismos, como representantes, para con sus electores-mandantes lo que, unido a la desviación del proceso crítico antes analizada, desde las cámaras legislativas hacia el proceso electoral, redunda en la idea de que el modelo de representación política actual se ha convertido en una *partitocracia.*

Pero esta concentración de poder en los diputados, que a su vez se encuentran sujetos a una disciplina de partido, cuya dirección política se determina de una manera altamente jerarquizada desde las ejecutivas, obedece en gran medida a un factor de naturaleza jurídica. Y es que la representación política, a pesar de tener muchas de las características de lo que hemos dado a llamar «representación colectiva», también alberga un elemento esencial de la representación privada:, más concretamente, de la representación legal: su obligatoriedad[17].

Se suele catalogar al sufragio como un «derecho político»[18], y dada su estrecha relación con la institución misma de la representación, se extiende esa concepción de derecho también al hecho de estar representado. Sin embargo, retrotraigámonos al concepto mismo de representación, consistente, dado X que representa a Y, en que las acciones de X, en nombre de Y, afectan a Y en su esfera personal y vital (ya sea económica, política, social o cultural). Así, toda ley que se aprueba en sede parlamentaria, toda decisión gubernativa proveniente de un Gobierno que deriva de una composición (y acción) parlamentaria, afecta a todos y cada uno de los ciudadanos, hayan participado o no en las elecciones, haya resultado su elección como ganadora o no, o incluso si su opción no ha superado los límites para obtener representación parlamentaria.

Si algo diferencia a la representación voluntaria de la legal (forzosa) es la voluntad del representado de otorgar esa capacidad al representante. En función de esta cualidad, podemos afirmar que la representación política se encuadra en el marco de la representación legal, donde ni siquiera se garantiza que entre los representantes resultantes tras unas elecciones se encuentre la opción por la que una persona aleatoria se haya podido decantar.

---

16 Algunos casos citados en EFE, Agencias, 28 de junio de 2012, accesible en http://www.20minutos.es/noticia/1524136/0/congreso/disciplina-de-partido/saciones/

17 Se podría discutir sobre si el elemento de obligatoriedad (o representación forzosa) se da también en otros tipos de representación colectiva, por ejemplo en la sindical, donde los acuerdos alcanzados por los sindicatos, materializados en convenios colectivos, afectan al conjunto de los trabajadores de ese sector, o del global, pero eso no quita que el elemento de obligatoriedad, característico de la representación legal, exista.

18 Artículo 23.1 CE, en relación con el 1.2 CE, y artículo 68.5 CE, entre otros.

En definitiva, es este elemento de obligatoriedad, de sujeción forzosa a la acción de los representantes políticos electos, la que confiere a estos una posición exclusiva, una intermediación forzosa en la acción política, una posición de poder difícilmente revocable[19]. En este sentido, nos encontramos con un sistema donde se propician y favorecen concentraciones de poder en lo que BOURDIEU llamó un «monopolio de profesionales»[20]

Por tanto, si el sistema de «pesos y contrapesos» establecido en la regulación jurídica de todo el procedimiento electoral, del proceso legislativo, o de las relaciones entre los poderes del estado es ineficaz, no ya sólo para mantener una efectiva separación de poderes, sino para garantizar unas mínimas bases democráticas, quizás sea el momento de introducir cambios en la teoría, en la práctica y hasta en el lenguaje, empezando por substituir esa arcaica y falaz *separación* del poder por una real y efectiva *distribución* del mismo.

3. SOBRE LA «DES-REPRESENTACIÓN POLÍTICA»

3.1. Definición

Podemos ensayar una definición sencilla de la *desrepresentación política* como *la potestad subjetiva para revocar a voluntad un mandato representativo político, legalmente conferido a un órgano o institución, materializado a través de sus miembros en el ejercicio de su cargo.* Como este trabajo versa sobre el proceso legislativo, dicha desrepresentación se llevaría a cabo sobre los miembros que componen una cámara legislativa, resultantes de un proceso electoral.

A partir de esta primigenia definición, es necesario desarrollar una serie de características que la contextualicen y la adapten a las especiales circunstancias del proceso legislativo y a la mecánica y dinámicas de lo que, en definitiva, constituye el funcionamiento y la organización de un estado democrático y de derecho.

3.2. Características

a) **Voluntaria.** En una situación de partida y de facto, donde la representación política se da por hecha, independientemente de la voluntad del representado, la potestad y el acto de la desrepresentación debe circunscribirse dentro del ámbito de libertad política de la persona. Sólo manteniendo y respetando esta capacidad se completaría la noción primigenia de la representación, en su histórico aspecto contractual social.

---

19 Incluso contando con la influencia de los partidos sobre la acción de los diputados, si un partido expulsa a uno de sus diputados, éste no deja de serlo, sino que pasa a engrosas las filas del «grupo mixto» como «independiente», si no se cambia a otro grupo parlamentario ya existente.

20 BOURDIEU, P. 1982. La representación política. Elementos para una teoría del campo político. *Actes de la Recherche en Sciences Sociales*, Nº 36-37, p, 4

b) **Activa.** El acto de desrepresentación debe consistir en una acto de voluntad positivo, de hacer. Esta característica se impone por la propia naturaleza de la acción política a gran escala y por la necesidad de manifestación expresa de voluntad. Se incardina dentro del juego de presunciones dentro de los procesos legislativos o de la acción de gobierno, íntimamente ligada con el aspecto obligatorio de la representación política y con la presunción de interés general que se atribuye a la conformación de mayorías. También está relacionada con la discrecionalidad con la que actúan los representantes políticos, que no están obligados legalmente a consultar cada acción o decisión a sus representados.

c) **Discrecional.** Lo que significa que queda al criterio de cada individuo cuándo y cómo participar. Éste puede hacerlo de manera puntual o continuada, siendo ésta una potestad permanente, pero no obligatoria.

d) **En tiempo real.** Dados los actuales cambios y progresos en las tecnologías de la comunicación, es posible la acción política directa, ciudadana, en pequeños márgenes de tiempo. Procesos que antes resultaban costosos, en tiempo y en recursos, como una votación a nivel estatal o la elaboración de textos entre muchas personas, hoy día se ven notoriamente simplificados y facilitados.

Estas características se observarán mejor en el punto 4, donde se proponen formulas y mecanismos concretos para la desrepresentación política.

3.3. Fundamentación jurídica

En el caso concreto del ordenamiento jurídico español, me centraré en dos líneas argumentales que justifican la necesaria habilitación de la desrepresentación política y la puesta en marcha de mecanismos efectivos para ejercerla.

En primer lugar, la remisión al bloque constitucional de Derechos Fundamentales, que se contiene en la Sección Primera del Capítulo II de nuestra Constitución, lo que le confiere una especial protección y garantía desde los poderes públicos. Es en el artículo 23 donde se reconoce a los ciudadanos el «derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal.

Del análisis sintáctico del fragmento entrecomillado, extraído directamente del citado artículo, se interpreta con meridiana claridad que, en la disyunción formulada a través de la conjunción «o», nos encontramos ante dos opciones alternativas y excluyentes: o bien se participa directamente, o bien por medio de representantes electos. Sin embargo, llama la atención que en la propia sinopsis[21] del artículo que aparece en la web del Congreso de los Diputados, elaborada por el profesor Raúl Casanova Usera en

21 Accesible en http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=23&tipo=2

2003 y actualizada por la Letrada de las Cortes Ángeles Escudero, la opción de participar directamente no aparece prácticamente desarrollada.

En dicha sinopsis se produce de manera continua una identificación entre el derecho de participación y el papel de los cargos electos. Es más, los nombrados autores citan la STC 51/1984 del 25 de Abril para afirmar que «mediante este tipo de participación –a través de representantes– el ciudadano contribuye a la formación democrática de la voluntad estatal, y ésta se produce *directamente* a través de la elección de representantes que forman los órganos en donde esa se expresa». En dicho fragmento rechina bastante que se utilice el adverbio «*directamente*» junto a «*a través de la elección de representantes*». Si lo que pretenden es resumir la participación directa, derecho conferido en el artículo 23, a la mera elección de representantes, nos encontramos ante una redundancia carente de sentido, ya que las dos opciones que se recalcan en el artículo se reducirían a la misma, siendo la participación pura y simplemente indirecta.

Es aún mayor la disonancia cognitiva que produce tal conceptualización del derecho de participación cuando se relaciona el artículo 23 directamente con el 1.2, que reza que la «soberanía reside en el pueblo, del que emanan los poderes del Estado. Si entendemos que la acción de emanar, la materialización de esa soberanía, se reduce a la elección de representantes y cargos, estaríamos equiparando los poderes del Estado a dichos cargos, una reducción *ad personam* que pone en peligro el propio concepto de soberanía y la relación de representación que de ella trae cuenta, algo que, por otra parte, es lo que ocurre actualmente.

Nos encontramos, por tanto, ante una cuestión de bastante calado interpretativo, donde la concepción hegemónica y predominante ha venido reduciendo el derecho de participación a la mera elección de representantes, redundando en la idea que he intentado transmitir antes, acerca de la obligatoriedad intrínseca a la institución de la representación política, hasta el punto de convertirla, a pesar de la percepción social, en una representación legal, y esto conecta con la segunda línea argumental.

En el amplio marco jurídico que regula los tipos de representación, como ya he mencionado con anterioridad, se considera que, para imponer cualquier tipo de representación, extrayéndola del catálogo de las voluntarias, es necesaria una valoración minusvalorada de la voluntad y la capacidad del representado, insuficientes para actuar por sí mismo. Los casos concretos de representación legal regulados en el ordenamiento jurídico establecen con claridad los criterios por los que se impone, sea legalmente o mediante sentencia judicial, una representación forzosa. Estos criterios se pueden resumir fundamentalmente en dos: la incapacidad o la ausencia.

Ejemplos de representación legal motivada por la incapacidad para obrar pueden ser la tutela, la curatela, la patria potestad o la asistencia en un proceso judicial. Por otra parte, la ausencia de un individuo motiva que otra persona deba actuar en su nombre, representando una voluntad que no puede manifestar debido a su ausencia, para aqué-

llos actos o negocios que no se puedan posponer al momento en el que aparezca. Como se puede comprobar, todo gira entorno a los elementos ya citados: voluntad y capacidad.

Si aplicamos estos criterios a la representación política de carácter forzoso, nos encontramos con dos argumentos que pueden justificarla.

En cuanto a la ausencia, tiene sentido pensar que, dada la dificultad para introducir a miles y millones de personas en una cámara legislativa, lo costoso de los desplazamientos y de los procesos de votación, es preceptiva la acción a través de representantes, que completen esa «ausencia por imposibilidad material», manifestando a través de la representación política la voluntad de los «ciudadanos ausentes».

Sin duda, esta motivación tiene todo el sentido del mundo, en el mundo en el que se redactaron las constituciones actuales o en aquél donde se diseñaron los sistemas parlamentarios representativos. Sin embargo, con las actuales herramientas tecnológicas de la comunicación, es posible hacer presentes a los ausentes, por muchos que sean, en cualquier situación geográfica o habitáculo espacial, por muy pequeño que sea. Los límites físicos, espacio-temporales, han dejado de ser un impedimento que justifique la necesidad de participar políticamente a través de representantes. Es más, a raíz de las reformas de las Cortes Valencianas (2006), replicada después en el propio Congreso de los Diputados (2012), los parlamentarios ya pueden votar los proyectos y proposiciones de Ley desde su casa, en caso de estar de baja. Si un diputado ausente por enfermedad no necesita de una nueva representación para subsanar su puntual ausencia en una votación, sino que puede hacerlo de forma telemática, huelga comenzar a plantearse si la misma lógica no debería aplicarse a la participación directa ciudadana.

En cuanto a la falta de capacidad, y a pesar de posiciones como la de Sartori[22], es jurídicamente indefendible y científicamente imposible certificar que los cargos electos disponen de una mayor capacidad, por su naturaleza o por el proceso de su elección, para desempeñar funciones como proponer y votar textos legales. Si, como se desprende de la SSTC 148/1986 de 25 de noviembre y 127/1991, de 6 de junio, las normas de acceso al cargo público son generales y abstractas, y no *ad personam*, si no existen mayores requisitos para resultar electo en un proceso electoral que ser mayor de edad y no incurrir en una expresa inhabilitación penal, en teoría, cualquier persona que cumpla esos requisitos estaría en disposición de ejercer su *desrepresentación* política y actuar efectivamente por sí mismo.

Concluyendo, podemos afirmar que la capacidad y la ausencia, el conocimiento y los límites espaciales o temporales, han dejado de ser barreras a la participación directa ciudadana o, al menos, ya no pueden considerarse excusas que, otrora, se consideraban insalvables. El desarrollo de las tecnologías de la comunicación, en especial Internet,

22 *Cfr,* SARTORI, G., 1999, p.2

habilitan al ejercicio *desrepresentado* de la política, redefiniendo el sentido del Estado Democrático.

4. MECANISMOS DE ACCIÓN POLÍTICA DESREPRESENTADA. INCIDENCIA DE INTERNET EN EL PROCESO LEGISLATIVO

Estamos viendo cómo se empiezan a dar pasos en la utilización de Internet para la participación política ciudadana. Existen experiencias interesantes en Brasil[23], en Estonia[24], en Islandia[25] e, incluso, en España[26], pero todas ellas siguen funcionando desde la dinámica de la representación[27]. Sin embargo, existen ya fórmulas novedosas que sí inciden en la idea de utilizar la Red como medio de ejercer la *desrepresentación*, participando de una manera desintermediada en el proceso legislativo.

4.1. La elaboración y proposición colaborativa de leyes

En realidad, ya existe en España (y en otros países) la posibilidad de elaborar colaborativamente un texto con pretensiones de convertirse en ley, bajo la figura de la Iniciativa Legislativa Popular (en adelante *ILP*). El problema, como he comentado en el caso de Islandia, es que el resultado de esa iniciativa debe pasar varios trámites parlamentarios (primero por una Comisión delegada y luego, en caso de pasar el primer trámite de control, por una votación plenaria en el Congreso)[28].

Frente a este bloqueo sistemático, surgen propuestas novedosas que buscan abrir el proceso de elaboración y proposición de textos legales. Como ejemplos se puede citar

23 Gabinete Digital del estado de Rio Grande do Sul https://gabinetedigital.rs.gov.br/

24 País pionero en permitir el sufragio por Internet o usando el teléfono móvil.

25 La Constitución Ciudadana de Islandia, elaborada en la red por una muestra sorteada entre ciudadanos voluntarios.

26 El diputado de Equo-Compromís, Joan Baldoví, puso su escaño a disposición para trasladar el resultado de una votación abierta en Internet sobre la Ley de Transparencia.

27 La única de las experiencias citadas que suponía, en cierto modo, un acto de desrepresentación política es el proceso de elaboración de la Constitución islandesa. Sin embargo, el resultado de este proceso tenía que ser validado por el parlamento, por lo que no se completaba el ciclo completo y, en última instancia, el poder de decisión residía en los cargos electos, como ocurre, por ejemplo, con la Iniciativa Legislativa Popular en España.

28 Una de las últimas ILP presentadas, la de la Plataforma de Afectado por la Hipoteca, llegó a alcanzar un respaldo ciudadano de más de 1.400.000 firmas, pero no pasó el trámite parlamentario sin ser completamente modificada y transformada en la nueva Ley 1/2013 de Protección de los Deudores Hipotecarios, fuertemente criticada.

el punto sobre *Wikilegislación*, dentro del programa del Partido X[29]. Sin embargo, el proceso que se presenta, si bien pretende ampliar los márgenes participativos de la actual *ILP,* permitiendo la deliberación y la enmienda ciudadana también sobre los proyectos de Ley (los que propone el Gobierno)[30], deja en manos de sus promotores la capacidad de aceptar o rechazar (motivadamente) esas enmiendas. Así mismo, no contempla explícitamente una ampliación de las materias sobre las que actualmente se puede formular una ILP, aunque tampoco limita expresamente la acción de *wikilegislación* materias concretas, quedando ese ámbito un tanto vacuo.

Más amplia y abierta es la propuesta contenida en el *informe*[31] que el grupo *Democracia Digital Andalucía* entregó a la Dirección General de Participación de la Junta de Andalucía como parte del proceso colaborativo para la redacción de la futura Ley de Participación andaluza. Dicha propuesta, denominada Acción Legislativa Popular (*ALP*), se recoge en el punto 1.5.8.3. del informe, dentro del catálogo de herramientas de participación de carácter vinculante para los poderes públicos, lo que da una idea de la preocupación por los tradicionales bloqueos parlamentarios que suelen sufrir las iniciativas populares.

Es de destacar que la *ALP* sí que contempla ampliar las materias susceptibles de ser legisladas, al mismo tiempo que dispone un proceso de elaboración abierto y descentralizado, donde son los propios ciudadanos los que van validando la progresiva construcción del texto, superando mediante el alcance de *quorums*, las diferentes fases de proposición, deliberación, corrección y votación, sin que la potestad de aceptar o rechazar enmiendas recale en ningún grupo reducido, sino en el total de la población mayor de edad.

4.2. La Votación directa de las leyes

Quizás la máxima expresión en el ejercicio de la *desrepresentación* política sea la potestad de votar directamente los proyectos y proposiciones de Ley que se presentan en una cámara legislativa. El efecto primero que se produce con esta medida es la implantación automática de un sistema de *veto* ciudadano sobre las propuestas de los

29 http://partidox.org/wikigobierno-y-wikilegislaciones-o-elaboracion-de-legislacion-participativa-y-transparente/

30 Nada se dice de las «proposiciones de Ley», que corresponden a las Cortes Generales, aunque no sabemos si por desconocimiento de que el ordenamiento jurídico español distingue entre ambas figuras o por no considerar adecuada la enmienda de proposiciones que emanan de las cámaras legislativas estatales o de las CC.AA.

31 Accesible en http://openkratio.org/index.php/democracia-digital-en-la-ley-andaluza-de-participacion/

partidos, revolucionando los tradicionales mecanismos de *pesos y contrapesos* de la teoría parlamentaria clásica.

La fundamentación del derecho a votar directamente las leyes nace del concepto de soberanía popular[32] y se presenta como máxima expresión de ésta,

Existen diferentes formulaciones del mecanismo del voto directo de las leyes, con sensibles diferencias. Por un lado tenemos el concepto de *democracia líquida*[33], asumido como propuesta por la red de Partidos Pirata, donde, además de promulgar el derecho a votar directamente las leyes, se consagra la posibilidad de poder delegar el voto en cualquier persona, independientemente de que sea o no cargo electo, en lo que supone una vuelta de tuerca a la institución de la representación política, haciéndola más dinámica y cambiante, de ahí el apelativo de «líquida».

Por otro lado, en España surgió la iniciativa de base jurídica *Democracia 4.0*[34], consistente en una petición amparada por el derecho fundamental consagrado en el artículo 29 CE. La peculiaridad de esta iniciativa es que toma como base la legislación ya existente y, en un acto de «hackeo»[35] jurídico, la dispone de manera que, con la sola modificación del Reglamento del Congreso, pueda encajar perfectamente en nuestro derecho.

Es es esta iniciativa donde se puede observar con más claridad la noción de *desrepresentación* y el papel fundamental de Internet en su aplicación. Dada una votación cualquiera en una cámara legislativa, esta iniciativa propone que cualquier ciudadano pueda votarla utilizando su firma digital, ya sea desde su ordenador de casa o desde puestos establecidos *ad hoc* en edificios públicos. Para el cómputo de los votos, establece que, dado un censo español con 35 millones de votantes y un Congreso con 350 diputados, el voto de 100.000 personas equivale al peso de un escaño, lo que no implica que por cada 100.000 votos directos deje de votar un representante, sino la disminución proporcional del peso del voto de todos los representantes en función del número de votos directos registrados[36].

Se observa, pues, el mecanismo de la *desrepresentación* de la siguiente manera: dada una composición determinada de un parlamento, surgida de unas elecciones, los miembros de ese parlamento representan, una vez constituido, al conjunto de los ciudadanos (votasen o no, ganase su opción o no), y lo que allí se decida en función de unas reglas de mayorías afectará al ámbito vital de todos y cada uno de ellos. Sin embargo, cada

32 En España, artículo 1.2 CE.

33 Una explicación más detallada en http://www.democracialiquida.org/

34 JURADO, F, «Democracia 4.0; desrepresentación en el voto telemático de las leyes». Revista Internacional de Pensamiento Político, vol. 8, 2013, pp. 119-138.

35 Fundamentación jurídica de la iniciativa en http://demo4punto0.net/es/node/4

36 Sistema explicado más en profundidad en JURADO, 2013, p 121, y simulador disponible en http://demo4punto0.net/es/node/3

ciudadano tendría la potestad de intervenir en cualquier votación, detrayendo su cuota alícuota de soberanía y, en ese momento, *desrepresentándose* para actuar directamente. Así se contempla, de una manera mas gráfica, que, siendo el punto de partida, por defecto, una situación de representación (que o se altera si el ciudadano no actúa), el hecho de votar directamente significa dejar de estarlo mediante un acto de voluntad positivo.

Este sistema no acaba con la representación política, no se contrapone a la misma, pero la altera cosiderablemente en varios aspectos:

a) Por un lado, establece un derecho de veto real de la ciudadanía sobre sus representantes, posibilitando una acción de fiscalización y de rendición de cuentas inmediata, en tiempo real. Esto reduce la discrecionalidad con a que se toman las decisiones, a sabiendas del largo horizonte temporal que trascurre entre elección y elección. Esto puede forzar, a su vez, a que los diputados realicen mejor su trabajo y se esfuercen más en explicar las leyes que producen, a sabiendas de que, independientemente de la mayoría que ostenten, pueden ser rechazadas.

b) Por otro lado, permite la conformación de mayorías sobre temas puntuales, con lo que quita peso a las filiaciones políticas de las que resultan las mayorías en unas elecciones. Esto haría que una persona pudiese votar puntualmente de forma diferente a la que lo hace su partido, sin tener que elegir a otro diferente, ajustando más la voluntad popular sobre el tema en concreto, y no sobre criterios más abstractos como la identidad cultural o la autoadscripción a un marco categorial ideológico.

c) También permite que las personas que no participaron en unas elecciones, o cuyos representantes no salieron electos (lo que supone varios millones de personas), puedan seguir participando en la vida política.

d) De cara a la acción de los *lobbys* o grupos de presión, diseminar la toma de deciisiones entre millones, en lugar de centralizarla en pocas personas, previene la coacción y la compra de voluntades, lo que reduciría males como el clientelismo, el tráfico de influencias o lo que se conoce como «la puerta giratoria».

En definitiva, se volvería a desplazar el proceso crítico antes mencionado hacia el Poder Legislativo, hacia la acción y hecho de legislar, quitándole peso al proceso electoral, reforzando la componente de *accountability,* al mismo tiempo que, mediante la participación, se podría combatir esa sensación (realidad) de lejanía de las instituciones y desapego (o desafecto) popular hacia las mismas.

En este sentido, el papel de la tecnología es clave, no sólo por materializar la desintermediación, sino por su potencialidad a la hora de sistematizar y presentar la información, por la posibilidad de implementar herramientas digitales que faciliten la deliberación y construcción colaborativa de textos. Pero, para ello, debe ir acompañada de unas posibilidades de acceso reales y masivas y de un programa esppecífico de alfabetización digital, con el objetivo de no abrir brechas ni crear *ghettos* tecnológicos. Al mismo tiempo, es necesario que estos procesos y proyectos se desarrollen desde lo pú-

blico, utilizando a la Adminiistración Electrónica y programando en código abierto, de manera que la transparencia y la capacidad de control de los procesos sea real y no se escape (ni externalice).

En nuestro país hay ya varias experiencias que permiten ser optimistas respecto al soporte tecnológico de los procesos de *desrepresentación*. Entre ellas podemos destacar a la plataforma *Agora Voting*[37] para las votaciones, o a herramientas de discusión orientadas a la producción colaborativa de leyes, como *Inwik*[38].

5. BIBLIOGRAFÍA

Alcazan y otros, 2012, *Tecnopolítica, Internet y R-Evoluciones,* Icaria.

Bourdieu, P. 1982. La representación política. Elementos para una teoría del campo político. *Actes de la Recherche en Sciences Sociales*, Nº 36-37.

Cotta, M., 1983: *Representación política*, en N. Bobbio, N. Matteuci y G. Pasquino, Diccionario de política (ed. española: J. Arico y J. Tula), Madrid, Siglo Veintiuno Editores, pp. 1425-1433.

Democracia Digital Andalucía (varios autores), 2013: *#InformeDDA, recuperado el 30 de enero desde http://openkratio.org/index.php/democracia-digital-en-la-ley-andaluza-de-participacion/*

Ferrajoli, L, 2007: *Principia Iuris. Teoria del diritto e della democrazia*, Roma-Bari, Laterza & Figli, 2 vols.

Ferrándiz, J. P. (2013). *No nos representan.* Blog de Metroscopia en El País. Recuperado el 30 de enero de 2014 desde http://blogs.elpais.com/metroscopia/2013/02/no-nos-representan.html

García Guitián, E., 2001: Crisis de la representación política: las exigencias de la política la presencia, en *Revista de Estudios Políticos*, núm. 111, enero-marzo, pp. 215-226.

Günther, R. (1989). Leyes electorales, sistemas de partidos y élites, *Reis: Revista Española de Investigaciones Sociológicas, nº* 47, pp. 73-106.

Hobbes, Th., 1980: *Leviatán*, trad. M. Sánchez Sarto, México, Fondo de Cultura Económica.

Jurado, F., 2013; Democracia 4.0; desrepresentación en el voto telemático de las leyes. *Revista Internacional de Pensamiento Político,* vol. 8, pp. 119-138.

37 https://agoravoting.com/

38 https://www.youtube.com/watch?v=1g_SQ8YRyRE

Lifante Vidal, I., (2009). Sobre el concepto de representación. *DOXA, Cuadernos de Filosofía del Derecho*, 32. ISSN: 0214-8676 pp. 515-519.

Pitkin, H. F., 1985: *El concepto de representación*, trad. R. Montoro Mero, Madrid, Centro de Estudios Constitucionales (original inglés de 1967).

Sartori, G. 1999: En defensa de la representación política, en *Claves*, núm. 91, pp. 2-6.

ARE SOCIAL MEDIA CHANGING PARTY POLITICS? BROKERS AMONG THE MEMBERS OF THE CATALAN PARLIAMENT TWITTER NETWORK

Marc Esteve i del Valle
Rosa Borge Bravo
UOC_IN3

ABSTRACT: This article focuses on a longitudinal (January/February/March 2014) analysis of the Twitter following-follower network of the members of the Catalan parliament. Our main objective was to find out if Twitter triggered new forms of political leaderships. In that regard, based on a network analysis we discovered that due to the working milieu that these networks reflect, the high reciprocity between the nodes of the network and their clustering structure, our networks unleash the appearance of brokers who, being different from the party leaders, are bridging the different political clusters. Regarding the particularities of the brokers of the network, our study finds that the position of centrality in the twitter networks does not depend on the political official role a parliamentarian holds, their official position within the party or the visibility at the Parliament. Neither the sociodemographic profile nor the Internet activity produces a difference. Only two variables seem to characterise differently the brokers in this network: the majority of brokers belong to CIU or ERC and have a Facebook account. Nevertheless, the results are not statistically robust probably due to the different level of analysis of our dependent (network level) and explanatory variables (individual level). Further research is required to understand the factors accounting for brokerage in the Catalan parliament's twitter network.

KEYWORDS: Catalan parliament, twitter network, network brokers, political leadership, betweeness centrality.

1. INTRODUCTION

Twitter was Launched in March 21, 2006 by Jack Dorsey and on December 31, 2013, it had an Average Monthly of Active Users of 241 million (Twitter, 2013), an increase of 30% year-over-year.

As a social media, Twitter[1] introduces new forms of political participation and deliberation. Such social networking service offers the potential to deliver conventional

1 It is an online social networking website and microblogging service that allows users to post and read text-based messages of up to 140 characters, known as «tweets». It gives its users the

forms of discourse to a wider audience (Saebo, 2011) while personalizing the communication flows up to a levels that previously where never reached in Politics. Moreover, Twitter gives voters the 'chance of entering into a real online dialogue with the representatives' (Mackay, 2010: 23), enhance relationship building (Briones et al., 2011) and allow individual citizens to make, contribute, filter and share content (Bechmann & Lomborg, 2012). Notwithstanding, it also puts pressure on parties' hierarchical structures (Gustafsson, 2012, p. 1,123) while blurring their classical strategy built on a sharp difference between their members and the public (Margetts, 2001; Gibson, Ward & Lusoli, 2003; Löfgren, 2003) and facilitating the direct contact between the public and parties' representatives (Golbeck, Grimes & Rogers, 2010; Missingham, 2010; Thamm & Bleier, 2013)

As we can see, a growing body of research has begun to examine the influence of social networking sites services on political communication from multiple angles. However, we believe that there is still a long way to go in understanding the effects that Twitter could have on the nature, characteristics and functions of the parliamentarians' public debate. More precisely, we believe that parties and politicians' appropriation and usage of social media have opened many questions about their effects on our Parliaments amongst which we would try to answer two: are the parlamentarians' twitter networks facilitating the appearance of new political leaderships and therefore paving the way for brokerage? Which are the factors behind the bridging behaviour of some parliamentarians? In this light, our objective will be to comprehend the characteristics and particularities of the parliamentarians' Twitter networks and the factors triggering the appearance of new internet-mediated forms of Parliamentarian political communication leaderships.

This study contributes to this research by exploring how Twitter was used by Catalan parliament representatives. Conceptually, we use the empirical study to weave together two strands of research. The first strand of research analyses different aspects related to the use that politicians do of Twitter which goes from their electoral usage (Tumasjan et al., 2010; Aragon, 2011; Barberá & Rivero, 2012) through the relations of network movements with political candidates (Esteve, forthcoming) until the parliamentarians use of Twitter (Golbeck, et al., 2010; Grant et al., 2010; Missingham, 2010; Verweij, 2012). The second strand argues that online interactions on Twitter may be analyzed by using the theoretical tenets of social network analysis in order to find out the structure of the network under analysis (Smith, et al., 2014) while emphasizing the analysis of the interdependence amongst the nodes over the role that they play individually (Newman, et al., 2006; Tsvetovat & Kouznetov, 2011). Indeed, this strand also points out that

opportunity to share short messages (tweets) and to respond to tweets (reply) or simply forward a tweet (retweet).

some types of networks pave the way for the appearance of brokerage (Burt, 2005) and it studies the characteristics and the role played by brokers[2] (González-Bailon & Wang, 2013) in bridging[3] (Putnam, 2000) the different clusters of the network.

The organization of the paper is as it follows. Next section introduces the Catalan case. Then we analyze the related work on online social networks, Twitter and political studies. We continue with details of the design of the research, the construction of variables and we state the research hypothesis to be tested. We then present the findings of our paper. Finally, we discuss the implications of these findings and outline potential avenues for future research in this area.

2. THE CATALAN PARLIAMENT AND TWITTER

Catalonia is a good case of study for several reasons: First, according to the CEO[4] figures an important part of the Catalan citizenry use the Internet (27,8%) and social networks (19,7%) to reach political information (CEO Third wave March April 2014).

Second, the appearance of the network movement 15-M (Castells, 2013), the economic crises together with the austerity measures, and the Catalan pledge for holding a referendum of independence[5], triggered a political context in which social media played a role as a socio-technical mean of political communication either for the citizenry or the representatives.

Third, the early social networking sites adoption by the Catalan Parliament and its members. In that regard, the Catalan Parliament initiated on 17 March 2009 the project «Parliament 2.0» consisting on «adapting through social media the Parliament to the new active role of users» (Ernest Benach, 2010). Moreover, the ratio of Catalan parliamentarians with Twitter in 2013 was 84.5% far higher than those figures reached by the Spanish parliament (52.6%), the Spanish Senate (33.06%), the German Bundestag

2 According to Burk a broker (bridge in Burks' terms) is «a (strong or weak) relationship for which there is no effective indirect connection through third parties. In other words, a bridge is a relationship that spans a structural hole»(Burk, 2005, p. 24).

3 According to Putnam: «Bridging social capital refers to social networks that bring together people of different sorts, and bonding social capital brings together people of a similar sort»(Putnam, 2000 cited in Norris, 2002, p. 3).

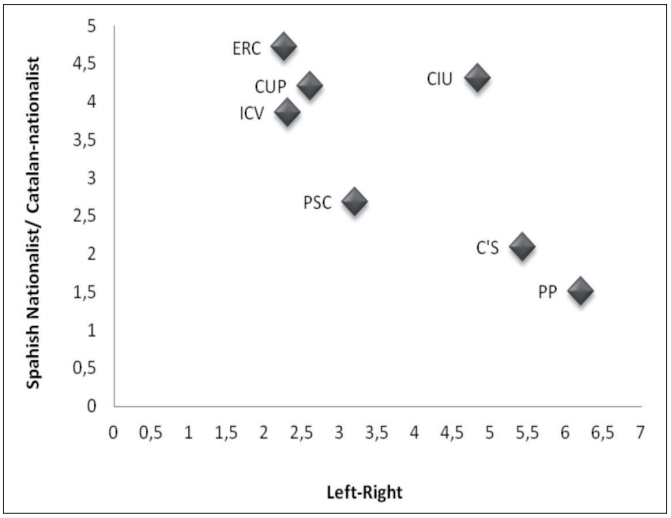
4 CEO is a Catalan governmental center for public opinion studies.

5 In that regard on 12 December 2013 President Artur Mas announced an agreement reached by CIU, ERC, ICV-EUiA and CUP regarding the date (9 November 2014) and the questions (Do you want Catalonia to be a state? Voters will be asked, and if so: Do you want it to be independent?) for holding the referendum.

(31,61%), the French Senate (42,07%), the UK house of commons (72,3%) but somehow behind those of the US Senate (100%) and the House of Representatives (90%).

Fourth, the Catalan party system characteristics. On the one hand, It is a fragmented system with a wide variety of fringe and medium-size parties. In fact, after the elections of 25 November 2012 we find seven parties in the Catalan parliament: CiU[6] (50 seats), ERC[7] (21 seats), PSC[8] (20 seats), PP[9] (19 seats), C's[10] (9 seats), ICV-EUIA[11] (13 seats) and CUP[12] (3 seats). On the other, the Catalan party system is distributed along two main ideological cleavages (see graphic 1), the left-right and the Spanish Nationalist-Catalan Nationalist. The following graphic (see Graph 1) place the Catalan parties in this two axes:

Graph 1: The position of the Catalan parties on the Catalan political spectrum according the CEO respondents



Source: Second round of the CEO surveys (20 June 2013); N=2000; Simple answer %.

6 CIU is a Catalan nationalist centre-right party.

7 ERC stands for Republican Left of Catalonia and it is a leftwing independetist party.

8 PSC is the Socialists' Party of Catalonia and it is federated with the Spanish Socialist Party.

9 PP is the Popular Party of Catalonia, which is member of the Spanish Popular Party, a rightwing and Spanish nationalist party.

10 C's stands for 'Citizens' and it is a relative new centrist and against Catalan nationalism party.

11 ICV-EUIA is a leftwing party self defined as eco-socialist and an autonomous part of the Spanish United Left (IU).

12 CUPs stands for 'Candidacies of Popular Unity' and are an extreme left and independentist coalition.

Last but not least, several studies have already showed that Social Media contributed to equalize the opportunities for political communication among Catalan parties as well as the Catalan citizenry participation through these channels for parties of varied sizes and with different political positions (Balcells and Cardenal, 2013; Esteve and Borge, forthcoming).

2.1. Previous studies

Since their inception, the political communication of parties' and their representatives have mutated hand in hand with the changes in society unleashed by the appearance of new forms of communication technologies. However, the controversy regarding parties' organization and communication was given a boost with the appearance of the internet and ICTs. The Web and, specifically, the spread of Social Media, are shaping the way parties, representatives, members and their electoral arena organise their relationships.

The effects of the Internet on political parties have been deeply studied by political scientists. In that sense, some authors pondered about the organizational rearrangements triggered by parties' adoption of ICTS on parties' relations with their members and the electorate (Gibson and Ward, 1999; Margetts, 2001; Heidar and Saglie, 2003; Vissers, 2009) while others studied the factors facilitating and differentiating parties' appropriation and use of Internet based technologies (Römmele, 2003; Padró-Solanet and Cardenal 2008; Cardenal 2011).

By the same token, the relation between social media and parties has been analysed from different points of view which goes from the citizen opinion about the use that parties should do of social media (Lynch and Hogan, 2012) through the social media erosion of parties' hierarchies (Gustafsson, 2012; Skovsgaard & Van Dalen, 2013) until the political communication personalization effect of social media (Klinger, 2013). Notwithstanding, in this section we will show that there is still a long way to go in studying the internet mediated social networks of the parliamentarian members and the implications that these new forms of communication among parliamentarians have for parliaments deliberation and the parties' political communication strategies developed in this particular milieu.

We will review the literature dealing with these two aspects: a) how parties' and their representatives are using social media specifically, twitter; b) how social network analysis is able to find out the structure and the characteristics of that network and its nodes.

2.1.1. Parties' and their representatives use of Twitter

Twitter has become a new channel for information and communication within political parties or among representatives and their voters. Literature on parties and

politicians' uses of Twitter has rapidly increased after Barack Obama's victory in 2008 presidential elections yet it has mainly been axed on comprehending the role of Twitter in electoral arenas. In this manner, while Tumasjan et al, showed that the analysis of the sentiments derived from tweets was a good predictor of elections' results (Tumasjan et al, 2010) Jungherr et al, and Aragón et al, demonstrated the impossibility to predict elections' results with a twitter sentimental analysis (Jungerr et al, 2011; Aragón et al, 2012). On the other hand, regarding the effects of Twitter political usage on electoral campaigns, Barberà and Rivero argued that during the 2010 Spanish national elections the citizens with a higher party identification monopolized the majority of the Twitter conversations (Barberá & Rivero, 2012, p. 5) and Aragón et al. as well as Labella showed that during the electoral campaigns the level of interaction among the members of different parties is very low (Aragón et al, 2012; Labella, 2012). More recently, Monterde et al, (forthcoming) and Esteve (forthcoming) have studied the political effects and interactions of the appearance and development of network movements (YoSoy132) on the Mexican political landscape and the 2012 presidential campaign.

On the other hand, even if the majority of the investigations have focused on the electoral arena, it is also true that some research has been conducted on the parliament representatives' use of Social Media. First, some authors have studied the factors behind the parliamentarians' adoption of twitter. In that sense, Lessen and Brown found that while socio-demographic factors did matter to the adoption of Twitter, the internet usage and the members' years in Congress have not any influence (Lassen & Brown, 2010). All the way around, Chi and Yang found that socio-demographic factors did not have any effect on parliamentarians Twitter adoption (Chi and Yang, 2010). In this same regard, Williams and Gulati stated that party pertinence and campaign resources are drivers of twitter adoption (Williams & Gulati, 2010). Second, other researchers have analyzed the parliamentarians' different behavior on twitter by analyzing the content of their tweets. In this light, Golbeck, Grimes and Rogers argued that Congresspeople were primarily using Twitter to disperse their own information but that they also use it to contact directly with citizens (Golbeck, Grimes and Rogers, 2010). In this same light, Small stated that Canadian party leaders mainly used Twitter to broadcast official party information (Small, 2010). Third, another stream of research focused on comprehending the characteristics of parliamentarians' Twitter interactions by studying their retweets and mentions. In this sense, Grant et al, pointed that there are two factors influencing the number of times a politician would be likely to be retweeted, his/her number of followers (the more followers a politician has the more likely to be retweeted) and their Twitter behavior (politicians who themselves were more likely to engage in conversational tweeting were also more likely to be retweeted) (Grant et al, 2010). In this same line of research, Conover et al, observed that retweet graphs reproduce the known partisan segregation in the online world while via the reply graph ideologically opposed individuals interact with each other (Conover et al, 2011) and Thamm and

Bleier demonstrated that retweets have a professional use while replies have a personal connotation[13]. Last but not least, more recently some researchers started to analyze Twitter relations among representatives from a social network analysis perspective pointing out the nature and characteristics of these affiliation networks (Verweij, 2012; Smith et al, 2014) and stressing the difference between the following-followers and mentions social networks in Twitter (Yoon & Park, 2014).

In a nutshell, we believe that our study could be very useful in order to provide empirical support to understand social media networks and the way how social media are changing politics. Furthermore, we think that the analytical tools used in this article could also be applied to analyze other parliamentarian and social networks. Last but not least, we hope that this analysis contributes to better comprehending the effects of political interactions on Twitter for the parliamentarians, their political groups and the parliamentarian deliberation.

2.1.2. Social Network analysis and the study of social media networks

Human beings have been part of social networks since our earliest days. People connect with others through social networks formed by kinship, language, trade, exchange, conflict, citation and collaboration. Social networks are created whenever people interact, directly or indirectly, with other people, institutions and artefacts (Hansen et al, 2011). Simply put, a «network is a set of nodes (such as people, organizations, web pages or nation states) and a set of relations (or ties) between these nodes» (Hogan, 2011, p. 2)[14].

Social network theory and analysis is a relatively new set of ideas and methods largely developed over the past 80 years. As a paradigm network analysis began to mature in the 1970s. In 1969 Stanley Milgram published his Small World experiment, demonstrating the colloquial «six degrees of separation»[15] (Travers & Milgram, 1969) and in 1973 Mark Granovetter published the landmark «the Strength of Weak Ties»[16]

13 More precisely these authors pointed that «within the communication behavior of MPs replies and retweets serve different purposes that are time-variant. While the retweet activity is more constant, reply activity tends to increase towards evening and also slightly on weekends. In both cases we see a growth of replies associated with typical leisure times (Thamm and Bleier, 2013, p. 2).

14 B.Hogan, Analyzing Social Networks Via the Internet: http://individual.utoronto.ca/berniehogan/Hogan_SAGE_Internetworks_RC1.pdf [Retrieved 13 March, 2014].

15 This experiment shows that everyone is six or fewer steps away, by way of introduction, from any other person in the world, so that a chain of «a friend of a friend» statements can be made to connect any two people in a maximum of six steps.

16 In this book Granovetter showed empirically and theoretically how the logic of relationship formation led to clusters of individuals with common knowledge and the 'weak ties' links beween these clusters.

(Granovetter, 1973). Then between the eighties and 2000 there was an explosive growth in number of network studies in different fields such as personal network studies (Wellman, 1979), the interconnectedness of corporate boards (Mizruchi, 1982) or the study of political networks (Knoke, 1990).

Nevertheless, increasing computational power and the dawn of the Internet ushered in the second major shift in network thinking: massive datasets could be gathered and analyzed in reasonable time frames (Hogan 2007: 1). On the one hand, authors such as Newman, Barabási and Watts focused on explaining the structure and dynamic of networks (Newman et al, 2006). In this same regard, Mislove (2009) and Tsvetovat & Kouznetov (2011) depict some of the tenets of the Social Network Analysis as well as the main characteristics of graph metrics in order to analyze social networks. On the other, there was a group of authors that emphasized some specific aspects of the network analysis such as the role of social networks in information diffusion and contagion (Paranyushkin, 2012; Bakshy et al, 2012) or the role played by brokers in bridging or bounding (Putnam, 2000) the social network clusters (Burt, 2005; González-Bailon & Wang, 2013). Last but not least, more recently some researchers have pointed out particular characteristics of the technical study of social networking sites such Twitter (Hansen et al, 2011) and Facebook (Hogan, 2011) while others have started to map Twitter conversations (Smith et al, 2014) and to point out some specific characteristics such as the fact that politicians' networks in Twitter are generally clustered with political affiliation groups of the ruling party and the opposition parties (Yoon & Park, 2014).

In a nutshell, in this article we will use all the theoretical and practical resources outlined above in order to explain the main characteristics of the Twitter network of the members of the Catalan Parliament and to find out the brokers of this network.

2.2. Research design, construction of variables and hypotheses

In this research we want to test if the Catalan parliamentarians' Twitter network paves the way for brokerage and to find out which are the factors behind the bridging behaviour of some Catalan parliamentarians. Formally we will test the following hypotheses:

H1: Given the high density of the Catalan parliamentarians' Twitter network, its high reciprocity, its clustering structure and the particular working milieu that it reflects, we expect the appearance of structural holes and therefore brokers.

H2: The Catalan parliamentarians who are young, highly educated, highly active on the Internet and parliamentarian works and belong to the ruling party, are more likely to be the bridges of the Catalan parliamentarians' twitter network.

In order to test these hypotheses empirically we will, first of all, find out who are the bridges of the Catalan parliamentarian Twitter network. For doing so, we will manually compile a list containing the usernames of the members of the Catalan Parliament on Twitter. Then we will use the NodeXL program to gather the data of our

Twitter network in a longitudinal perspective (13-01-2014; 24-02-2014; 24-03-2014) and to find out the brokers (Betweeness[17] centrality) of the Catalan parliamentarians' Twitter network. Lastly, we will visualize the network maps using the Gephi program.

On the other hand, once we will know the bridges of those networks we will carry out regression analyses to ascertain which are the factors explaining brokerage in the Catalan parliament Twitter network. The model will be run over the 115 members of the Catalan Parliament with Twitter accounts (85% of the parliamentarians). Our independent variables in the model include 5 dimensions:

a. Socio-demographic characteristics (age, educational level, gender)
b. Internet behaviour (having Facebook or a blog) and twitter activity (average tweets per day between 13th January and 24th March 2014).
c. Parliament activity (number of the commissions in which the parliamentarians participate and the number of their interventions in these commissions and in the plenary sessions).
d. Political position at the Parliament (role at the Parliament's commissions and at the parliamentarian group) at the party (party's president) or being a mayor.
e. Electoral characteristics such as party belonging and the number of legislatures at the Parliament (up to three).

2.3. Results

2.3.1. Network Analysis

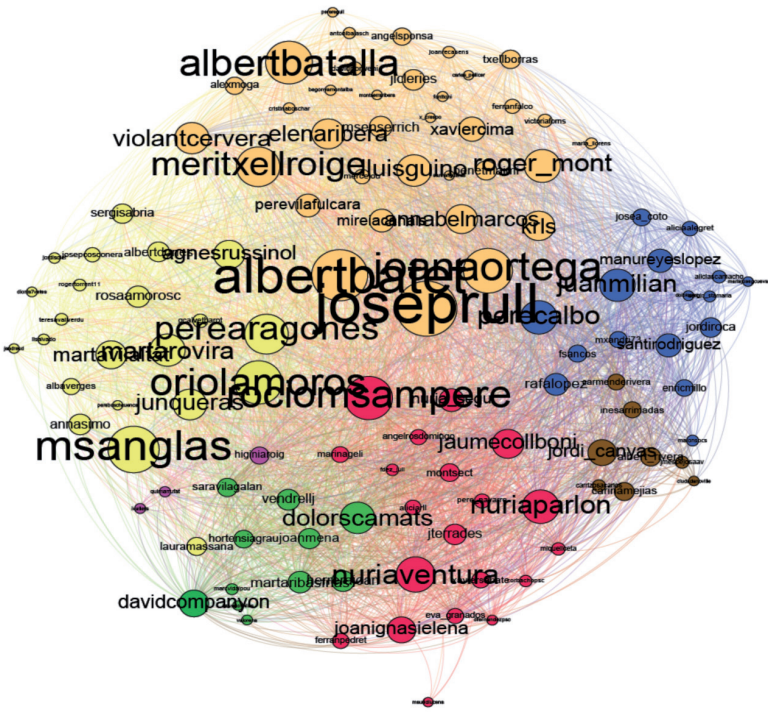
From the Network Analysis of the three Following-Followers Twitter networks of the Catalan deputies with Twitter could be observed different results: First, in our case study a selected group of 115 people created three Twitter networks of 4,447 (January 2014), 4287 (February 2014) and 4326 (March) relations. The maximum geodesic distance (diameter) of the three networks is three, which means that a maximum of three steps is needed to cross the network. The average distance of the three networks is 1.5 indicating that the average distance between the users is 1.5 steps. Moreover, the average density of the three networks is 0.32. This shows that 32 per cent of the total possible relations is realised. Although the density in all the networks is low, the short distances make it possible to easily connect to others.

Second, as it can be seen from Figure 1, Figure 2 and Figure 3, the three networks could be classified as being Tight Crowd and Affiliation networks. In this light, they are

17 Hansen, Shneiderman & Smith define the Betweneess Centrality such as «a measure of how often a givern vertex lies on the shortest path between two other vertices» (Hansen, Shneiderman & Smith, 2010:40).

Tight Crowd Networks for they have between 2-6 groups, a high level of interconnectivity, few isolates (Smith et al, 2014:8) and they are affiliation[18] networks because they respond to the internet-mediated relations web by the Catalan representatives in a particular milieu, the Parliament of Catalonia. Furthermore, it can be stated that the Tight Crowd Networks facilitate the appearance of structural holes[19] and therefore brokers who will bridge the different communities.

Figure 1: The Following-Follower Twitter Network of the Catalan deputies (January 2014)



*The nodes of the Nework are the 115 deputies with Twitter account

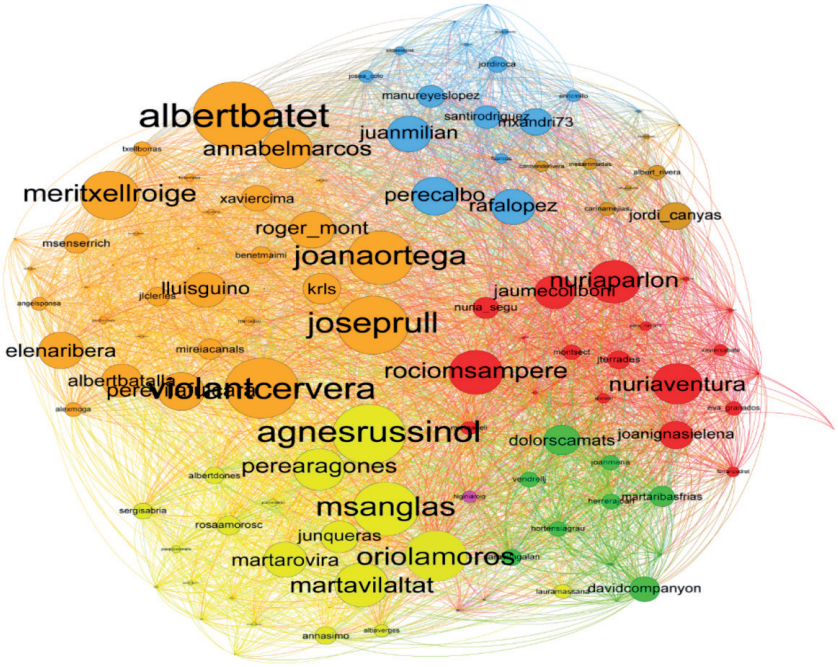
**The Size of the nodes is equivalent to their Betweeness Centrality in the Network

***The colour of the nodes is equivalent to the political party that they pertain: Orange (CIU), Yellow (ERC), Red (PSC), Blue (PP), Green (ICV), Brown (C'S) and Violet (CUP)

18 Newman defines the affiliation network such as a «network of actors connected by a common membership in groups of some sort, such as clubs, teams or organizations» (Newman, 2001, p. 3).

19 According to Burk a structural hole is: «A potentially valuable context for action, brokerage is the action of coordinating across the hole with bridges between people on opposite sides of the hole, and network entrepreneurs or brokers, are the people who build the bridges» (Burk, 2005, p. 18).

Figure 2: The Following-Follower Twitter Network of the Catalan deputies (February 2014)



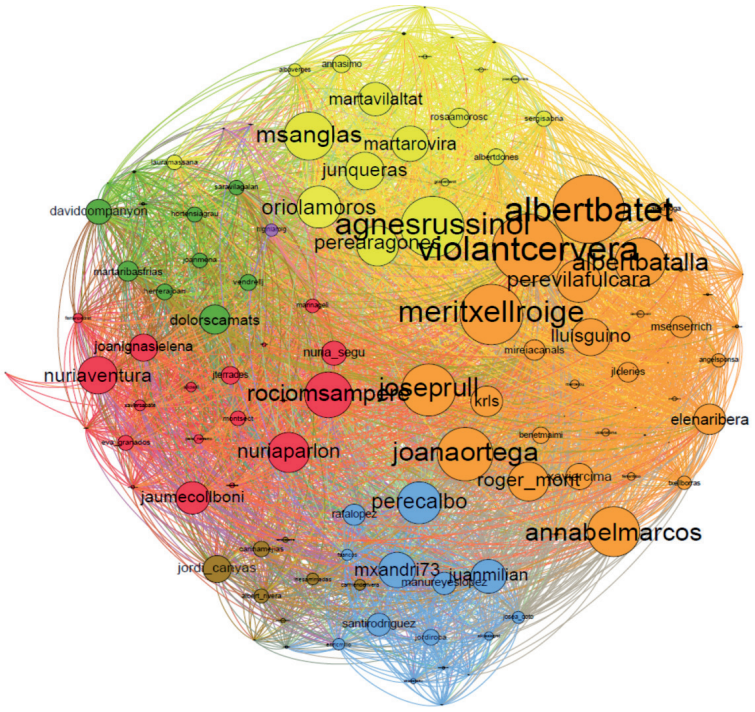
*The nodes of the Nework are the 115 deputies with Twitter account

**The Size of the nodes is equivalent to their Betweeness Centrality in the Network

***The colour of the nodes is equivalent to the political party that they pertain: Orange (CIU), Yellow (ERC), Red (PSC), Blue (PP), Green (ICV), Brown (C'S) and Violet (CUP)

****The position of the clusters in the three networks is given by the Force Atlas 2 algorithm. That means that the variation of the clusters' position in the network (left-right) must not be considered for the analysis.

Figure 3: The Following-Follower Twitter Network of the Catalan deputies (March 2014)



*The nodes of the Nework are the 115 deputies with Twitter account

**The Size of the nodes is equivalent to their Betweeness Centrality in the Network

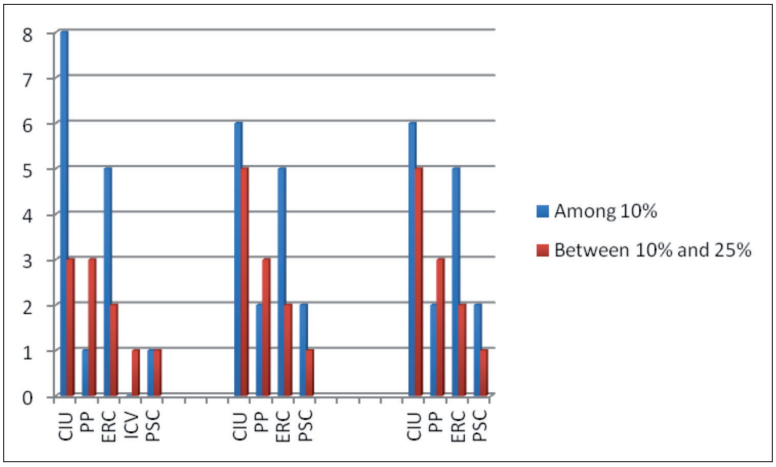
***The colour of the nodes is equivalent to the political party that they pertain: Orange (CIU), Yellow (ERC), Red (PSC), Blue (PP), Green (ICV), Brown (C'S) and Violet (CUP)

Third, our results in the analysis of the Reciprocated-Vertex-Per-Ratio of the nodes show an average of 0.5 (January), 0.51 (February) and 0.51 (March) which means that the following demands were reciprocated in the 50% of the cases (in average). These results can be aligned with those found by Young and Park (2014) therefore corroborating that the politician's Following-Followers relations may be much more influenced by internal social pressure than the other type of politician's networks (mentions and replies).

Fourth, with respect to the Left-Right and Nationalist cleavages from Figures 1, 2 and 3 it can be clearly observed the existence of these two dimensions. In that light, in the nationalist cleavage we observe the parties that consider themselves as Catalan nationalist parties and those that are not Catalan nationalist (PSC, PP, ICV, C's). On the other hand, with respect to the Left-Right cleavage we also observe the dimension which gathers the left parties (PSC, ERC, ICV and CUP) and the right ones (CIU, PP and C's).

Fifth, with regard to the broker position of the Catalan parliamentarian groups we should highlight two aspects: on the one hand, the strong longitudinal stability of the number of brokers of each parliamentarian political group (Figure 5). On the other, the low political relevancy of the brokers of the network. More precisely, our data shows that among the 25% of the brokers of the network only 4 of them occupy a relevant political position in their parties[20].

Figure 4: Number of brokers for each political party of the Catalan deputies' Following-Follower Network (January/Februrary/March)



*The Y axis represents the number of deputies and the X axis the different political parties for the three periods of analysis (From left to right: January/February/March)

**The blue line means the total number of brokers for each political party among the 10% of them with highest betweness centrality

***The red line means the total number of brokers for each political party among the 10 and 25% of them with highest betweness centrality

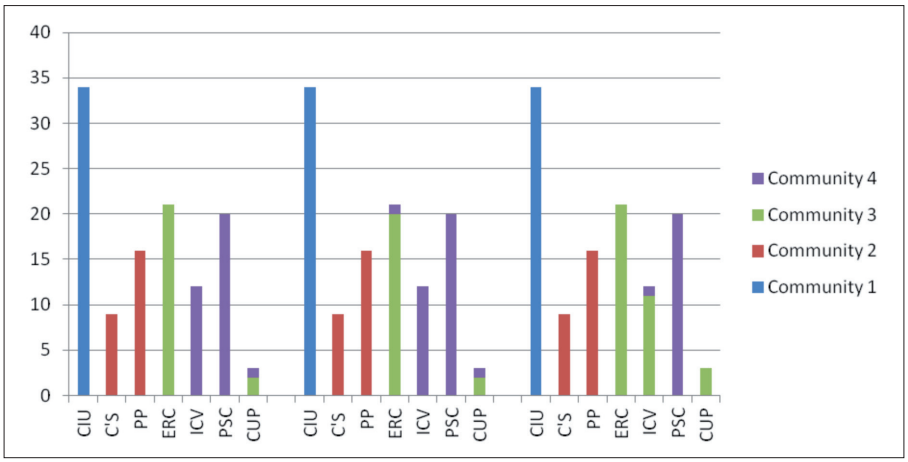
Last but not least, regarding the modularity[21] of the networks (Figure 4) the results show the existence of 4 clusters. Cluster 1 (CIU) and cluster 2 (C's+PP) show a high cohesiveness and longitudinal stability in comparison with clusters 3 and 4 (which are

20 @junqueras- president of ERC and who is among the 10% of the brokers in the three periods of time. @dolorscamats –Vice-President of ICV- who is between the 10 and 25% of the brokers in January.
@joanaortega –Vice-President of the Catalan Government and @martarovira –Secretary of Organization of ERC- who are between the 10 and 25% of the brokers in February and March.

21 Modularity measures how well a network decomposes into modular communities. A high modularity score indicates sophisticated internal structure. This structure, often called a com-

a combination of ERC, PSC, ICV and CUP). More precisely, the highest variability between clusters comes with the isolation of the PSC members triggered by the modification of the stance of the ICV and CUP parliamentarians towards the PSC members. In that regard, it should be mentioned that during the period of time of our analysis the Parliament of Catalonia has adopted different resolutions regarding[22] the pledge of Catalonia to hold a referendum of Independence in which the position of the majority of the PSC members has been different of that adopted by those of ICV and CUP.

Figure 5: Clusters of the Following-Follower Networks of the Catalan deputies (January/February/March)



**The Y axis represents the number of deputies and the X axis the different communities of the political parties for the three periods of analysis (From left to right: January/February/March)

***The communities were created using the modularity algorithm of Gephi program

2.3.2. Explanatory Analysis

Multiple regression and logistic regression analyses have been carried out in order to test the explanatory power of the variables proposed in our model. In both cases the

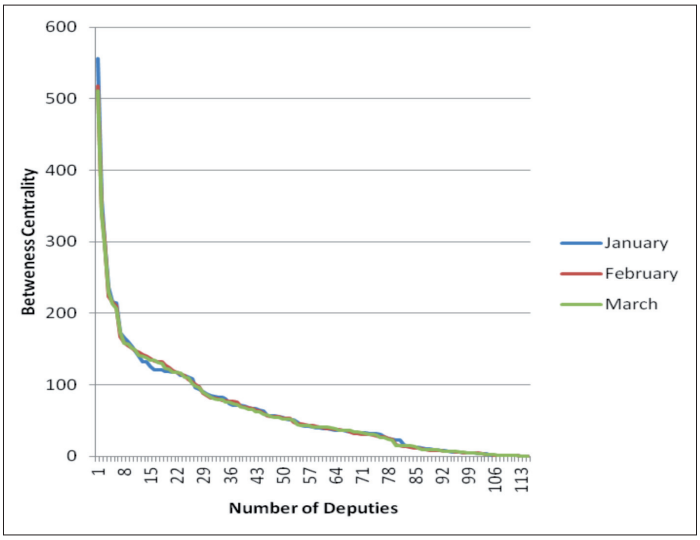
munity structure, describes how the network is compartmentalized into sub-networks. These sub-networks (or communities) have been shown to have significant real-world meaning.

22 In this sense we would like to mention the «Resolution 479/X of the Parliament of Catalonia by which it was agreed to submit to the Presiding Board of Congress the draft organic act delegating to the Generalitat of Catalunya power to authorize, call and hold a referendum on the political future of Catalonia».

dependent variable has been «Betweeness Centrality» (BC). For the multiple regression analysis we have kept the original format of the variable which ranks from 0 to 556,6.

But as we can see in Figure 6 the distribution of this variable is skewed towards the lowest limit following a similar distribution in the three months.

Figure 6: Betweeness Centrality distribution of the Catalan deputies (January/February/March 2014)



That is, only 22,6% of the cases have a high betweeness centrality (above 100) and therefore are the brokers in the network . 77,4% of the cases unfold a low level (below 100). Therefore we decided to carry out a logistic regression being 0= BC < 100 and 1= BC > 100.

Unfortunately in both analysis the proposed model of explanatory variables is not statistically significant, does not sufficiently account for the variance of the dependent variable in the case of multiple regression and does not improve the classification of the predicted values in comparison to the observed values in the case of logistic regression.

We suspect that the reason for the irrelevance of our explanatory model maybe lies in the different levels of analysis we are dealing with. The betweeness centrality is a network variable while the explanatory variables are individual variables. This suspicion is corroborated by other analysis we carried out taking individual features of the network as dependent variables. When we place the number of followers a parliamentarian's twitter holds (in-degree number) or the number of parliamentarian's twitters each parliamentarian is following (our-degree number) we find that the model is explanatory and statistically significant with three variables standing out as relevant and significant with negative coefficients: age, number of interventions to the plenary and the political position at the Parliament (spokesperson of the Parliament's group, president of the

Parliament's group or Parliament's secretary or vice-president). This means that when age decreases the following-followers number rises and when the number of interventions in the plenary and the political roles associated diminish the following-followers number rises as well. We have to take into account that the interventions in the plenary are performed by leaders within the party that hold relevant positions at the Parliament (Pearson's R= 0,385) but who are not necessarily central in the twitter network.

Setting aside the explanatory analysis which will be improved in next papers, the profile characteristics of the brokers are the following:

- The MPs who are brokers in the twitter network belong mainly to CIU (42,3%) and ERC (26,9%). Within the two parties more than 32% of the parliamentarians with twitter accounts are brokers.
- 40,9% of the women and 59,1% of the men have twitter accounts, but the percentage of brokers is quite similar among men (22,1%) and women (23,4%).
- The majority of the brokers have between 28 and 48 years old (76,95%), while only 23,1% have between 49 and 69 years old. Among the total number of twitter accounts the proportion is 61,7% and 38,2%, respectively.
- Regarding the level of education, 57,4% of the parliamentarians with twitter hold a bachelor's degree and 21,7% a masters' degree and 7,8% a PhD. But the proportion among brokers is 53,8%, 23,1% and 11,5%, respectively.
- 71,4% of the parliamentarians with twitter have Facebook accounts; 28,7% does not. Among brokers, 84,6 % have Facebook while 15,4% have not.
- 60% of the parliamentarians with twitter have a blog and 40% has not. Among brokers, 50 % have a blog while 50% have not.
- The mean of tweets per day among all twitter accounts is 3,68, and the mean among brokers is 3,38.
- The mean of the number of parliamentarian commissions which a member of the Parliament belong to is 4,51 among all twitter accounts and the mean among the brokers is very similar: 4,38.
- The mean of the number of interventions to the plenary among all twitter accounts is 47 and among brokers diminish to 41,6. The mean of interventions to the Parliament's commissions is 103 among the total and 73 among brokers.
- Incumbency seems to produce no difference: among the brokers 23,4% are new in the last legislature and 22,1% have been in the Parliament for one or two legislatures.

3. CONCLUSIONS

In this article we have observed that the Twitter relations among the Catalan parliamentarians give room for the appearance of new sorts of political leaderships.

In this light, the analysis of the three (January/February/March) following-follower networks of the Catalan parliamentarians revealed that their configuration trigger the appearance of the structural holes (Burt, 2005) and therefore brokerage. More precisely, our analysis permits us to state that due to the working milieu that these networks reflect, the high reciprocity between the nodes of the network and their clustering structure, our networks unleash the appearance of brokers who bridge the different political clusters.

Which is the profile of these brokers?. The parliamentarians who have the role of brokers are slightly younger (mean of 43 years) than the rest of parliamentarians with twitter accounts (mean of 45 years), the gender proportion is quite similar and they have a slightly higher educational level than the rest, but the differences are not significant. The biggest differences are found in two other dimensions: the government-opposition dimension and the disposition of a Facebook account. There is predominance of the party in government (CiU) and its ally in the Parliament (ERC) among the brokers. That is, 69,2% of the brokers belongs to CiU or ERC. Regarding Facebook, 84,6% of the brokers has a Facebook account.

Surprisingly, the political roles or appointees at the Parliament or within the party do not have an influence on the centrality in the twitter network, and even the number of interventions to the plenary or to the parliamentarian commissions or the number of commissions to which a parliamentarian belong are lower among the brokers than among the totality of twitter accounts. Therefore, the position of centrality in the twitter network does not depend on the political official role a parliamentarian holds, the official position within the party or the visibility at the Parliament.

Further research should be done to understand why and how the parliamentarians that are leaders and bridges of the twitter communication within the Parliament are not the official leaders of the party and do not hold important positions at the Parliament. In this regard, it is important to ascertain if the individual explanatory variables of our model must be complemented with more relational dimensions that account for the affinities in the following-follower twitter network of the Parliaments.

4. REFERENCES

Aragón, P., Kappler, K., Kaltenbrunner, A., Neff, J., & Laniado, D. (2012). Tweeting the campaign: Evaluation of political party strategies in Twitter for the 2011 Spanish national elections. Presented at the conference of *Internet, Politics & Policy 2012.* Oxford, OX: United Kingdom.

Bakshy, E., Rosenn, I., Marlow, C., Adamic, L. (2012). The role of social networks in information diffusion, In *Proceedings of the International World Wide Web Conference Committee* (IW3C2), Lyon: France.

Balcells, J., & Cardenal, Ana S. (2013). Internet and electoral competition: The case of Esquerra Republicana de Catalunya. *Revista Española de Investigaciones Sociológicas, 141,* 3-28.

Barberá, P., & Rivero, G. (2012). ¿Un tweet un voto? Desigualdad en la discusión política en Twitter [One tweet one vote? Inequality in the Twitter political discussions]. Document prepared for the 1st International Congress of Political Communication and Campaign Strategies. Madrid, MAD: Spain.

Benach, E. (2010). Política 2.0. Barcelona, BCN: Bromera.

Bechmann, A., & Lomborg, S. (2012). Mapping actor roles in social media: Different perspectives on value creation in theories of user participation. *New Media and Society, 15* (5), 765–81.

Boyd, D., & Nicole, E. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13* (1), 210–30.

Briones, R., Kuch, B., Brooke, L., & Yan, J. (2011). Keeping up with the digital age: How the American Red Cross uses social media to build relationships. *Public Relations Review, 37* (1), 37–43.

Burt, R. (2005). Brokerage & closure: An introduction to social capital (1st Edition). New York, NY: Oxford University Press.

Cardenal, Ana S. (2011). Why mobilize support online? The paradox of party behaviour online. *Party Politics, 19* (1) , 83–103.

Castells, Manuel. (2012). Networks of outrage and hope: Social movements in the Internet age. Cambridge: Polity Press.

Centre d'Estudis d'Opinió. (2014). *Baròmetre d'opinió política (BOP). 1a onada 2014* [Barometer of political opinión. 1st wave 2014]. Retrieved from http://www.ceo.gencat.cat/ceop/AppJava/pages

Chi,F., & Yang,N. (2010). Twitter adoption in Congress. *Review of Network Economics, 10 (1),*1-49.

Congressional Research Service. (2013). *Social networking and constituent communications: Member use of Twitter during a two-month period in the 111th Congress* (*7-5700*, R41066). Washington, DC: Glassman,M.E., Strauss,J.R., & Shogan,C.J. Retrieved from http://www.fas.org/sgp/crs/misc/R41066.pdf

Conover, M., Ratkiewicz, J., Francisco, M., Gonçalves, B., & Flammini, F. (2011). Political polarization on Twitter. *In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*, Barcelona: Spain.

Esteve, M. (forthcoming, 2014). El movimiento YoSoy132, Twitter y la contienda presidencial mexicana de 2012: De la indignación a las redes [The mouvement YoSoy132 , Twitter and the 2012 Mexican presidential campaign: From the indignation to the networks], *Revista de Estudios Latinoamericanos, 34.*

Esteve, M., Borge, R. (forthcoming, 2014). Abriendo brechas: centralización de las decisiones e interacción online en CIU, ERC y el PSC [Opening gaps: centralization of the decisions and online interaction in CIU, ERC and PSC]. *Revista de Internet, Derecho y Política, 17.*

Gibson, R., & Stephen, W. (1999). Party democracy on-line: UK parties and new ICTs. *Information, Communication and Society, 2* (3), 340–67.

Gonzalez-Bailon, S., & Ning, W. (2013) The bridges and brokers of protest campaigns using social media. Retrieved from SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2268165

Goldbeck, J., Grimes, J. M., & Rogers, A. (2010). Twitter use by the U.S. Congress. *Journal of the American Society for Information Science and Technology*, 61(8), 1612–1621.

Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78* (6), 1360-1380.

Gustafsson, N. (2012). The subtle nature of Facebook politics: Swedish social network site users and political participation. *New Media and Society, 14* (7), 1,111–27.

Hansen, D., Shneiderman, B., & Smith, M. (2011). *Analysing social media networks with NodeXL*. (1st Edition). Burlington, MA: Elselvier.

Heidar, K., & Saglie, J. (2003). Predestined parties?: Organizational change in Norwegian political parties. *Party Politics, 9*(2), 219–39.

Hogan, B. (2007). *Analysing social networks via the Internet.* Draft article retrieved 15 May from http://individual.utoronto.ca/berniehogan/Hogan_SAGE_Internetworks_RC1.pdf

Hogan, B. (2011). Visualizing and interpreting Facebook networks. In Hansen, D., Shneiderman, B., & Smith, M. *Analysing social media networks with NodeXL*. (1st Edition). Burlington, MA: Elselvier.

Jungherr, A., Jurgens, P., & Schoen, H. (2011). Why the Pirate Party won the German elections of 2009 or the trouble with predictions: A response to Tumasjan, A., Sprenger, T., Sander, P., & Welpe, I. 'Predicting Elections with Twitter: What 140 Characters Reveal About Political Sentiment'. *Social Science Computer Review, 30* (2), 229-234.

Klinger, U. (2013). Mastering the art of social media. *Information, Communication and Society, 16* (5), 717–736.

Knoke, D. (1994). Political networks: The structural perspective. New York, NY: Cambridge University Press.

Labella, L. (2012). Las redes sociales en la política española: Twitter en las eleccions de 2011 [Social networks in Spanish Politics: Twitter in the 2011 elecions]. *Estudos de Comunicaçao, 11,* 149-164.

Lassen,D., & Brown,A. (2010). Twitter: The electoral connection? *Social Science Computer, ooo(oo),* 1-18. doi: 10.1177/0894439310382749

Löfgren, K. (2003, April). *Intra-party use of new ICTs - Bringing memberships back in?.* Paper prepared for ECPR Joint Sessions of Workshops, Edinburgh: Scotland.

Lynch, K., & Hogan, J. (2012). How Irish political parties are using social networking sites to reach generation Z: An insight into a new online social network in a small democracy, *Communication, 13*, 83–98.

Mackay, J. (2010). Gadgets, gismos, and the web 2.0 election. In J.A. Hendricks,J & Denton , R. (Eds.) *Communicator-in-Chief: How Barack Obama used new media technology to win the White House* (pp. 19-36). Lanham, MD: Lexington Books.

Margetts, H. (2001, April). *Cyber parties.* Paper prepared for ECPR Joint Sessions of Workshops, Grenoble.

Missingham, R. (2010). The Australian parliament in the twitterverse. *Australian Parliamentary Review, 25* (1), 3-16.

Mislove, A. (2009). *Online social networks: Measurement, analysis and applications to distributed information systems* (Doctoral Dissertation). Retrieved from http://www.mpi-sws.org/~amislove/publications/SocialNetworks-Thesis.pdf

Mizruchi, S. (1982). *The corporate board network.* Thousand Oaks, CA: Sage.

Monterde, A., Carrillo, R., Esteve, M., & Aragón, P. (forthcoming, 2014). #YoSoy132: ¿Un nuevo paradigma en la política mexicana? [#YoSoy132: A new paradigm in Mexican politics?. *In3 Working Paper Series.*

Newman, M., Barabási, A., & Watts, D. (2006). *The structure and dynamics of networks* (Eds.). Princeton, NJ: Princeton University Press.

Norris, P. (2002). The bridging and bounding role of online communities. *Press/Politics, 7* (3), 3-13.

Grant, W., Moon, B., & Grant, J. (2010). Digital dialogue? Australians politicians use of the social network tool Twitter. *Australian Journal of Political Science*, *45* (4) 579-604.

Padró-Solanet, A., & Cardenal, A.S. (2008). Partidos y política en internet: un análisis de los websites de los partidos políticos catalanes [Parties and policy in Internet: An analysis of the Catalan parties webpages]. *IDP Revista de Internet, Derecho y Política, 6*, UOC. Online journal. Retrieved from http://www.uoc.edu/idp/6/dt/esp/padro-solanet_cardenal.pdf

Paranyushkin, D. (2012). Informational epidemics and synchronized viral contagion in social networks. Retrieved from: http://noduslabs.com/publications/Synchronized-Contagion-Viral-Social-Networks.pdf

Pedersen, K., & Saglie, J. (2005). New technology in ageing parties: internet use in Danish and Norwegian parties, *Party Politics, 11* (3), 359–77.

Pew Research Center. (2014). *Mapping Twitter Topics Networks. From Polarized Crowds to Community Clusters*. Washington DC: Smith, A.M., Rainie, L., Shneiderman,B., & Himelboim.I.

Putnam, R. (2000). Bowling Alone: The collapse and revival of American community (1st Edition). New York, NY: Simon & Schuster.

Römmele, A. (2003). Political parties, party communication and new information and communication technologies, *Party Politics. Special Issue Party Politics on the Net, 9* (1), 7–20.

Saebo, O. (2011). Understanding twitter use among parliament representatives: A genre analysis. *Lecture Notes in Computer Science, 6847,* 1-12. Doi: 10.1007/978-3-642-23333-3_1

Small, T. (2010). Canadian politics in 140 characters: Party politics in the Twitterverse. *Canadian Parliamentary Review,* Fall 2010, 39-45.

Skovsgaard, M., & Arjen, V.D. (2013). Dodging the gatekeepers: social media in the campaign mix during the 2011 Danish elections. *Information, Communication and Society, 16* (5), 737–56.

Thamm, M., & Bleier, A. (2013). When politicians tweet: A study on the members of the German federal Diet. In ACM Web Science 2013. Paris, France. Retrieved from http://www.websci13.org/

Travers, J., & Milgram, S. (1969). An experimental study of small world problem. *American Sociological Association, 32*(4), 425-433.

Tumasjan, A., Timm, O., Sandner. P., & Welpe. I. (2010). Predicting elections with Twitter: What 140 characters reveal about political sentiment, In *Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media*, Germany , Menlo Park, CA: The AAAI Press, 178-185.

Tsvetovat, M., & Kouznetsov, A. (2011). *Social network analysis for startups* (1st Edition). Sebastopol, CA: O'Reilly.

Vergeer, M., Liesbeth, H., & Steven, S. (2011). Online social networks and microblogging in political campaigning: The exploration of a new campaign tool and a new campaign style, *Party Politics*, *19* (3), 477–501.

Verweij, P. (2012). Twitter links between politicians and journalists. *Journalism Practice, 6 (5-6),* 680-691. Doi: 10.1080/17512786.2012.667272

Vissers, S. (2009). *From preaching to the converted to preaching through the converted*. Paper presented for the ECPR Joint Sessions of Workshops, Lisbon: Portugal.

Ward, S., & Gibson, Rachel. (2009). European political organizations and the internet. Mobilization, participation, and change. In A. Chadwick and P. Howard (Eds.) *Routledge Handbook of Internet Politics*, pp. 25–39. Oxford: Abingdon, Oxford.

Ward, Stephen., Gibson, R., & Werner, L. (2003). Online participation and mobilisation in Britain: Hype, hope and reality, *Parliamentary Affairs, 56* (4), 652-68.

Wellman, B. (1979). The community question: The intimate networks of east Yorkers. *American Journal of Sociology, 85*(5), 1201-1233.

Williams,C.B., & Gulati,G.J. (2010). Communicating with constituents in 140 Characters or Less. *Working Papers*. Paper 43. Retrieved from http://opensiuc.lib.siu.edu/pn_wp/43

Yoon, H.Y., & Park, W.H. (2014). Strategies affecting Twitter based networking pattern of South Korean politicians: Social network analysis and exponential random graph model. *Quality and Quantity, 48 (1),* 409-423.

LA IDENTIDAD DIGITAL EN PROCESOS DE DEMOCRACIA ELECTRÓNICA. LA DESASTROSA EXPERIENCIA DE LA FIRMA ELECTRÓNICA BASADA EN CERTIFICADOS, EN MIFIRMA.COM

Javier Peña
Presidente de MiFirma.com

Ignacio Alamillo Domingo
Investigador del GRISC, Universitat Autònoma de Barcelona

RESUMEN: La democracia electrónica, en algunas de sus modalidades, presenta retos referidos a la autenticidad de las actuaciones realizadas y, en especial, en relación con la identificación de los ciudadanos que ejercitan su derecho. En el caso de la Iniciativa Legislativa Popular (ILP), la regulación actual, contenida en el artículo 7.4 de la Ley Orgánica 3/1984, de 23 de marzo, reguladora de la Iniciativa Legislativa Popular (LOILP), añadido por Ley Orgánica 4/2006, de 26 de mayo, autoriza que «las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente», referencia que debe entenderse realizada a la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE), que actualmente establece, en un enfoque tecnológicamente neutral, diversos tipos de firma electrónica. Sin embargo, el Acuerdo de 10 de mayo de 2012, de la Junta Electoral Central, aplica esta posibilidad de forma extraordinariamente restringida, e injustificadamente alineada con la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y la normativa de interoperabilidad.

El efecto de esta «regulación» es absolutamente desastroso en términos de efectiva participación: restricción de uso de casi todos los sistemas de firma electrónica, obligación de empleo de certificados admitidos por la Administración, imposición de formatos técnicos específicos, imposibilidad de uso de formas de identidad digital de la Web 2.0…; en definitiva, un régimen que en términos prácticos hacen casi inviable el ejercicio de este Derecho.

PALABRAS CLAVE: Firma electrónica, Certificado electrónico, Identificación electrónica, Democracia electrónica, Iniciativa legislativa popular.

1. INTRODUCCIÓN

La participación puede conceptualizarse como una nueva forma de institucionalización de las relaciones políticas, basada en una mayor implicación de los ciudadanos y sus asociaciones cívicas, tanto en la formulación como en la ejecución y control de las políticas públicas. Mediante la participación ciudadana se pueden desarrollar e implementar políticas más informadas y favorecer una mayor transparencia y responsabilidad de las Administraciones Públicas, generando así una mayor confianza en el gobierno y

las instituciones políticas, cuestión que redunda en el fortalecimiento de la propia democracia representativa (Prieto Martín, 2007).

Es posible afirmar, con Martí, que hoy en día estamos viviendo una nueva transformación, un proceso de progresiva implantación de mecanismos participativos que, al menos en un futuro inmediato, no aspiran a sustituir por completo el sistema representativo existente, heredado de las estructuras del siglo XIX, sino a complementarlo y enriquecerlo con una fuente mayor de legitimidad (Martí, 2008).

El gobierno electrónico y, más concretamente, la denominada administración electrónica supone un mejor acceso a la información, un estímulo del pluralismo y un incremento de la participación, dado que Internet sirve de impulso tanto a las nuevas como a las tradicionales vías de participación de la sociedad civil (Fernández Rodríguez, 2006). Por otra parte, Pindado ha caracterizado la participación con las notas de necesidad estratégica de buen gobierno, al tratarse de un derecho que precisa canales para su efectiva realización y que necesita planificarse (Pindado, 2005).

La participación se encuentra consagrada como principio constitucional en el artículo 9.2 de la Constitución Española, que establece la responsabilidad de los poderes públicos de «facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social», entre otras. Este principio se desarrolla en el artículo 23.1 de la Constitución, al determinase que «los ciudadanos tienen el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal». Planteado en estos términos, el derecho de participación tiene un matiz esencialmente político y dada su ubicación en el texto constitucional es un derecho fundamental y, por lo tanto, goza del máximo nivel de protección jurisdiccional (García Rubio, 2005). Puede materializarse en dos modalidades:

- Democracia representativa o participación indirecta, entre las que cabe destacar los partidos políticos (artículo 6), los sindicatos de trabajadores o las agrupaciones empresariales (artículo 7), las asociaciones (artículo 22), los colegios profesionales (artículo 36) y las organizaciones profesionales (artículo 52) como principales fórmulas constitucionalizadas.
- Democracia directa o semidirecta, entre las cuales podemos citar la participación en la educación (artículo 27), la participación de la juventud (artículo 48), el derecho de petición a las Cámaras (artículo 77), el ejercicio de la iniciativa legislativa popular (artículo 87), la participación a través de referéndum (artículo 92), la audiencia de los ciudadanos, directamente o a través de las organizaciones y asociaciones reconocidas por la ley, en el procedimiento de elaboración de las disposiciones administrativas que les afecten (artículo 105.2), la participación en la Administración de Justicia (artículo 125) y la participación en la Seguridad Social y en la actividad de los organismos públicos cuya función afecte directamente a la calidad de vida o al bienestar general (artículo 129).

A modo de definición, se puede indicar que la participación electrónica es toda actividad voluntaria de los ciudadanos que se encuentra encaminada a influenciar en la selección de los gobernantes o en la toma de decisiones públicas, que se canaliza o se produce a través de medios electrónicos o telemáticos, pudiendo diferenciarse cinco niveles posibles en la participación (Borge, 2005):

- Información: Divulgación de información a través de las webs y de los correos electrónicos. Elementos informativos: documentos varios, enlaces web, comunicados, convocatorias, anuncios, avisos, noticias, etc.
- Comunicación: Relación y contactos de manera bidireccional a través del correo electrónico y de espacios de comunicación habilitados en las webs. Elementos comunicativos: preguntas, sugerencias, demandas, quejas, comentarios, cartas, organización de convocatorias y reuniones, etc.
- Consulta: Formas que emplean los gobiernos, Administraciones, y organizaciones diversas para saber las opiniones de los ciudadanos o de sus miembros. Elementos consultivos: referendos, encuestas, sondeos, etc.
- Deliberación: Procesos de examen, evaluación, reflexión, debate y discusión sobre las decisiones, opciones y valores que impregnan cualquier tema o problema sociopolítico. Elementos deliberativos: foros, chats, espacios de debate, etc.
- Participación en decisiones y elecciones: Participación en elecciones: voto electrónico. Participación en una actividad orientada a la toma de decisiones; es decir, el resultado final es vinculante para las autoridades: referendos o encuestas vinculantes, debates o foros vinculantes, recogida de firmas para iniciativas legislativas o para iniciar consultas ciudadanas en los ayuntamientos, etc.

En este trabajo presentamos el funcionamiento práctico de una experiencia de participación democrática electrónica en decisiones y, en concreto, para la recogida de firmas en procesos de iniciativa legislativa popular.

En el caso de la Iniciativa Legislativa Popular (ILP), la regulación actual, contenida en el artículo 7.4 de la Ley Orgánica 3/1984, de 23 de marzo, reguladora de la Iniciativa Legislativa Popular (LOILP), añadido por Ley Orgánica 4/2006, de 26 de mayo, autoriza que «las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente», referencia que debe entenderse realizada a la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE), que actualmente establece, en un enfoque tecnológicamente neutral, diversos tipos de firma electrónica.

Sin embargo, el Acuerdo de 10 de mayo de 2012, de la Junta Electoral Central, aplica esta posibilidad de forma extraordinariamente restringida, e injustificadamente alineada con la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y la normativa de interoperabilidad.

El efecto de esta «regulación» es absolutamente desastroso en términos de efectiva participación: restricción de uso de casi todos los sistemas de firma electrónica, obli-

gación de empleo de certificados admitidos por la Administración, imposición de formatos técnicos específicos, imposibilidad de uso de formas de identidad digital de la Web 2.0…; en definitiva, un régimen que en términos prácticos hacen casi inviable el ejercicio de este Derecho.

2. LA INICIATIVA DE RECOGIDA DE FIRMAS ELECTRÓNICAS

Mifirma.com e IniciativaLegislativaPopular.es eran dos plataformas que nacieron para la recogida de firmas electrónicas para Iniciativas Legislativas Populares (ILP). Las motivaciones de cada una de ellas eran diferentes: mientras la primera tenía una motivación más activista y social, en cambio la segunda tenía más relación con el desarrollo de nuevas tecnologías y su impacto.

Gracias a la intervención de la empresa Tractis, se realizó un encuentro entre las dos plataformas, que decidieron fusionarse para aunar esfuerzos y conseguir mejorar una única plataforma de manera, que pudiera dar el mejor servicio, siempre gratuito.

Tractis fue el proveedor de identidad inicial de la nueva plataforma nacida de esta fusión, también en régimen de prestación gratuita de sus servicios, si bien, y debido a las restricciones impuestas por la Junta Electoral Central, dicho sistema debió ser sustituido por el empleo de @firma, la plataforma del Ministerio de Hacienda y Administraciones Públicas. Además de este servicio, también ayudó en uno de los aspectos más importantes, como es el encuentro de varios expertos en administración electrónica de reconocido prestigio que se involucrarían en el proyecto. Esto derivó en el nacimiento de una asociación que gestionaría la plataforma y que continúa hasta la actualidad.

Las primeras ILPs fueron un reto pues era la segunda experiencia en España después de la recogida de firmas para el proyecto «Defendamos el Trasvase. Recojamos un rio de firmas».

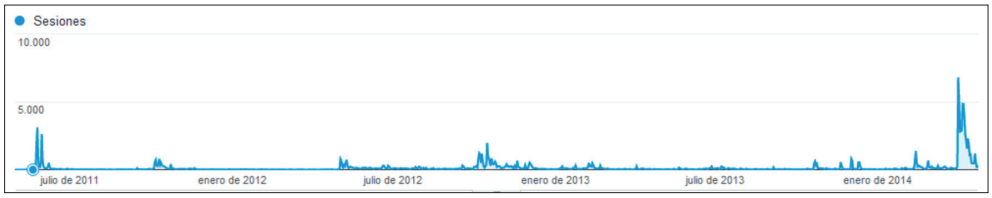
Respecto a los resultados logrados hasta la fecha, a continuación se muestran datos respecto a las diferente ILPs tramitadas:

NOMBRE ILP	Fecha Fin de Recogida	Número de formularios rellenos	Firmas Electrónicas Recogidas	Ratio
ILP de Personal de Guardia Civil	04/03/2012	398	26	7%
Iniciativa Legislativa Popular de regulación de la dación de pago, de paralización de los desahucios y de alquiler social	25/01/2013	21267	882	4%
Iniciativa Legislativa Popular sobre la reversión de la congelación de las pensiones en 2011	30/11/2012	312	32	10%
Iniciativa Legislativa Popular Por la Protección, Preservación y Conservación del Litoral Andaluz	26/07/2013	1070	55	5%
¡FIRMA! por la libre elección del sexo de los hijos	19/11/2013	391	10	3%

NOMBRE ILP	Fecha Fin de Recogida	Número de formularios rellenos	Firmas Electrónicas Recogidas	Ratio
Conmemoración del V Centenario de la Primera Vuelta al Mundo, Sanlúcar 2019-2022	03/05/2014	53	8	15%
Las pensiones a la Constitución. ¡Referéndum Ya!	01/08/2014	2726	140	5%
Ley para la Auditoria del Déficit de Tarifa Eléctrico	11/11/2014	3773	618	16%
Iniciativa Legislativa Popular de modificación de la Ley Electoral de Andalucía	09/06/2014	805	106	13%
Ley para la Separación de bienes en el matrimonio	23/01/2015	107	13	12%
Iniciativa Legislativa Popular por la Renta Básica Estatal	14/12/2014	296	44	15%
		31198	1934	6%

Como se puede ver, se trata en general de resultados más bien modestos, pero más importante aún es ver la relación entre los formularios cumplimentados por los firmantes y las firmas realmente generadas, ya que denota la dificultad de firmar electrónicamente.

Desde otra perspectiva, a 13 de mayo de 2014 la web de MifFirma.com había recibido 158.000 visitas, con 580.226 páginas vistas, como se puede ver en el siguiente gráfico:



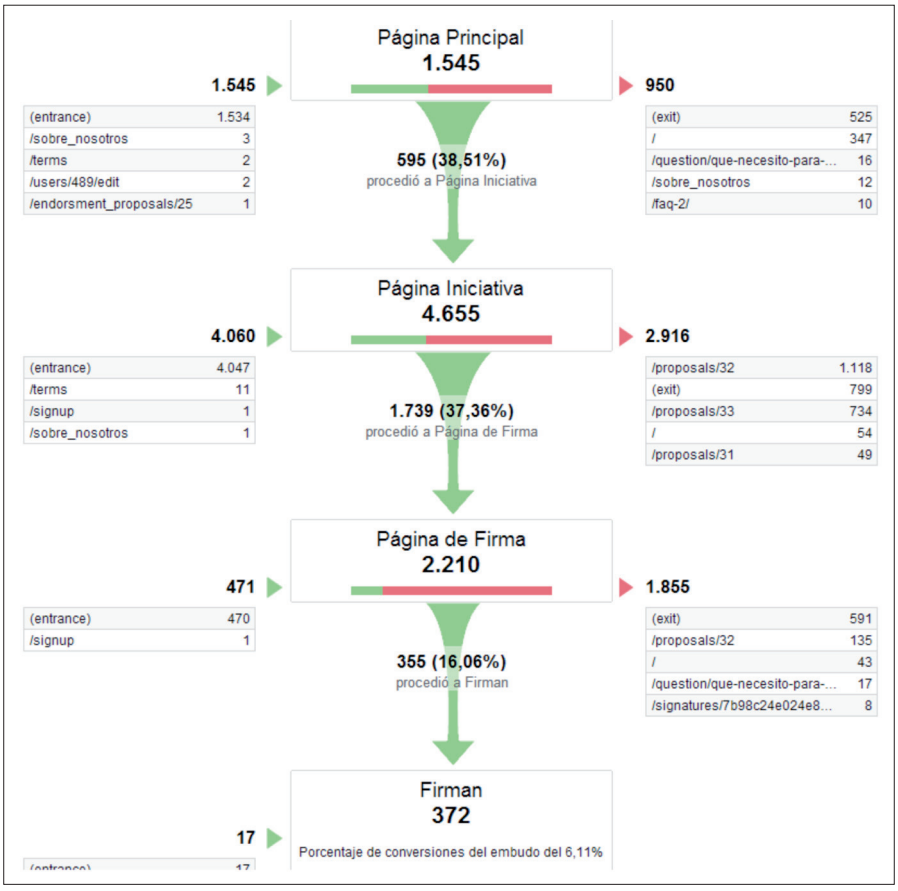
Uno de los datos más relevantes para medir la eficacia del sistema es la tasa de conversión, que nos informa del número de personas que visitan la web de MiFirma.com consiguen llegar a firmar.

En este sentido, desde el 1 de octubre de 2013 a 28 de febrero de 2014 la tasa de conversión ha sido del 3,72%, que como podemos observar es muy baja. Es cierto que hay que resaltar que cifras son muy variables, dependiendo del tipo de trámite y el momento de ejecución.

Por ejemplo, en el lanzamiento de la ILP de Auditoría Energética se ha logrado una tasa de conversión del 7,76%, mientras que en el lanzamiento de la ILP autonómica Reforma Ley Electoral, la tasa de conversión ha sido del 2,29%.

Podemos avanzar que la firma electrónica basada en certificados ha sido un fracaso, al menos a tenor de los resultados esperados.

Para detallar la problemática observada, podemos basarnos en el gráfico de embudo del mes de febrero de 2014, que se muestra a continuación:



Podemos partir de la página de la Iniciativa que se quiere firmar. Muchos de los accesos son directos a esta página (como se puede ver son 4.047 en el concepto de «entrance»), lo cual es debido a que el acceso a la página de la iniciativa en MiFirma.com se suele realizar desde la página web de la iniciativa de la comisión promotora.

Podemos observar que el 37% de las visitas han rellenado el formulario de manera correcta, con su DNI y datos personales para continuar. El resto de las visitas no han continuado por diversos motivos, entre los cuales podemos identificar:

- Falta de interés o desacuerdo con la iniciativa.
- Desconfianza en la plataforma.
- Simple curiosidad.

El problema comienza cuando se requiere proceder a generar una firma electrónica: de 2.210 intentos de firma con el certificado, recordemos que una vez que el formulario ya ha sido correctamente relleno con los datos personales del ciudadano, solo el 16% consiguen firmar.

¿Cuál es la razón que lleva a esta situación? Del estudio realizado, cabe entender que se trata, principalmente, de una cuestión técnica ligada al empleo de los certificados electrónicos, que enumeramos aquí:

- Necesidad de una máquina virtual de Java que funcione adecuadamente, que parece es el principal problema. La máquina virtual de Java es necesaria actualmente para poder realizar el proceso de firma en el navegador y a día de hoy existen pocas alternativas al respecto.
- En concreto, se han experimentado diversos incidentes de no funcionamiento del *applet* de @Firma debido a actualizaciones de Java, así como la necesidad de «desaprender» seguridad informática, porque para poder firmar frecuentemente hay que enseñar al usuario a desactivar las funciones de seguridad de los navegadores.
- Recordemos que además las *tablets* y teléfonos móviles no disponen de esta máquina virtual de Java y por tanto los ciudadanos no pueden firmar o deben realizar instalaciones complejas de aplicaciones adicionales para ello. Hasta un 30% de los ciudadanos que han accedido al servicio lo han hecho con estos sistemas.
- En cuanto al DNI electrónico, muchos ciudadanos piensan que el DNI electrónico les permitirá firmar pero cuando descubren que:
  - No se acuerdan del PIN.
  - No disponen de un lector de tarjetas.
  - No tienen bien configurado el driver del lector y los módulos criptográficos de la policía.
  - Descubren que el certificado que incluye el DNI electrónico ha caducado (lo cual se produce a los 30 meses, independientemente de la caducidad del DNI físico), si bien en este caso la Junta Electoral Central admite estas firmas siempre que se pueda determinar de forma indubitada su autenticidad.
- Simplemente no disponen de un certificado electrónico, o disponen del certificado de la FNMT-RCM, cuyo uso no es gratuito para MiFirma.com, lo cual no parece ser la mejor forma de promocionar este instrumento. Supone el 50% de los problemas reportado por los usuarios de la plataforma cuando ya se han decidido a firmar. En febrero de 2013, España había emitido más de 38 millones de DNI electrónicos. Esto significa que el usuario o no es consciente o tiene los problemas mencionados en el punto anterior. Esto nos hace ser conscientes del fracaso del DNIe como certificado de consumo por parte del ciudadano. También se puede comprobar con los datos del Ministerio de Industria donde menos de un 2% de los trámites están realizados con el DNIe.

Como se puede verificar, el uso de instrumentos como la firma electrónica avanzada basada en certificados, y más aún, en el DNI electrónico, constituye una verdadera barrera técnica a la firma electrónica de iniciativas legislativas populares, por lo que cabe criticar el Acuerdo de 10 de mayo de 2012, de la Junta Electoral Central, sobre el pro-

cedimiento para la verificación y certificación de las firmas de una iniciativa legislativa popular.

Dicho Acuerdo precisamente impone una serie de condiciones técnicas a la firma electrónica, entre las cuales podemos destacar las siguientes:

- Se establece un formato específico en XML para la representación de cada firma electrónica de una Iniciativa Legislativa Popular.
- La firma electrónica a efectos de la presentación de una iniciativa legislativa popular se entenderá válida siempre que sea una firma electrónica avanzada, basada en un certificado reconocido por las administraciones públicas y publicado en la sede electrónica del Instituto Nacional de Estadística https://sede.ine.gob.es, válido a la fecha de la firma.
- El XML con los datos del firmante según el esquema anterior deberá ser firmado siguiendo la política de firma de la Administración General del Estado definida en (OID: 2.16.724.1.3.1.1.2.1.8). Dentro de esta política se recomienda la firma en formato XADES, clase básica, *internally detached*.

3. CONCLUSIONES

Como se ha presentado, la firma electrónica de las Iniciativas Legislativas Populares a través de Internet presenta una gran cantidad de problemas técnicos ligados al uso de los certificados digitales.

El Acuerdo de la Junta Electoral Central es injustificadamente restrictivo, incluso a la luz de la aplicación de la legislación de Administración electrónica, a tenor de las escasas exigencias contenidas en la Ley Orgánica reguladora, y se debería modificar en el sentido de admitir otros tipos de firma electrónica adecuados.

Dichas condiciones, y en particular, las restricciones técnicas asociadas a la firma electrónica, impiden de forma clara la efectividad de las Iniciativas Legislativas Populares, algo claramente criticable a la luz de lo dispuesto en el artículo 7.4 de la Ley Orgánica 3/1984, de 23 de marzo, reguladora de la Iniciativa Legislativa Popular (LOILP), añadido por Ley Orgánica 4/2006, de 26 de mayo, autoriza de forma expresa la posibilidad de emplear cualquier sistema de firma electrónica para la recogida de firmas, cuando indica que «las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente».

Dicha referencia debe entenderse realizada a la Ley 59/2003, de 19 de diciembre, de firma electrónica, que prevé otras modalidades de firma electrónica que resultarían perfectamente aceptables en el ámbito de la Iniciativa Legislativa Popular, como muy correctamente ha puesto de manifiesto la doctrina, dado que el nivel de seguridad de una iniciativa no tiene porqué ser ni medio ni alto, y apostando incluso por la posibilidad del anonimato o de uso de seudónimos (Cotino Hueso, 2011).

Otros medios de firma electrónica podrían incluir el uso de claves concertadas y mecanismos no criptográficos, de la identidad digital en redes sociales y terminales móviles, o de la firma electrónica biométrica en *tablet*, incluso capturada presencialmente, de forma que se podrían sustituir los muy obsoletos pliegos sellados.

4. BIBLIOGRAFÍA

Borge Bravo, R. (2005): «La participación electrónica: estado de la cuestión y aproximación a su clasificación». IDP. Revista de Internet, Derecho y Política [artículo en línea]. Núm. 1. UOC.

Cotino Hueso, L. (2011): «La iniciativa ciudadana europea electrónica», en Cerrillo Martínez, A.; Peguera, M.; Peña López, I. y Vilasau Solana, M. (Coords.): *Neutralidad de la red y otros retos para el futuro de Internet*. Barcelona: Huygens.

— «El derecho a relacionarse electrónicamente con las Administraciones y el estatuto del ciudadano e-administrado en la Ley 11/2007 y la normativa de desarrollo», en Gamero Casado, E. y Valero Torrijos, J. (Coords.): *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Cizur Menor: Aranzadi Thompson Reuters.

Fernández Rodríguez, J.J. (2006): «La aprehensión jurídica de la democracia y el gobierno electrónicos», en Cotino Hueso, L. (Coord.): *Libertades, democracia y gobierno electrónicos*, Granada: Comares.

García Rubio, Fernando (2005): «La participación ciudadana en la Administración local y las nuevas tecnologías. Un análisis de su régimen jurídico», en *La participación ciudadana en las grandes ciudades*, Madrid: Dykinson.

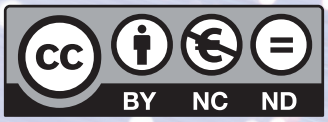
Martí, J.L (2008): «Alguna precisión sobre las nuevas tecnologías y la democracia deliberativa y participativa» [artículo en línea], en *La democracia electrónica* [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. Núm. 6. UOC.

Martín Delgado, I. (2010): «Identificación y autenticación de los ciudadanos», en Gamero Casado, E. y Valero Torrijos, J. (Coords.): *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Cizur Menor: Aranzadi Thompson Reuters.

Pindado, F. (2005): «La participación no se improvisa», en *Talleres de participación y ciudadanía – Materiales*, Revista de Estudios Locales, Núm. 87. Madrid.

Prieto Martín, P. (2007): «Sistemas avanzados para la participación electrónica municipal: ejes conceptuales para su diseño», en Cotino Hueso, L. (Coord.): *Democracia, participación y voto a través de las nuevas tecnologías*. Granada: Comares.

Valero Torrijos, J. (2007): *El régimen jurídico de la e-Administración: El uso de medios informáticos y telemáticos en el procedimiento administrativo común (2ª ed)*. Granada: Comares.



Internet, Derecho y Política
Una década de transformaciones

Actas del *X Congreso Internacional Internet, Derecho y Política (IDP 2014)*

ISBN: 978-84-697-0826-2

Para citar la obra, por favor, utilicen las siguientes referencias indistintamente:

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2014). *Internet, Derecho y Política. Una década de transformaciones*. Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio, 2014. Barcelona: UOC-Huygens Editorial.

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2014). *Internet, Law & Politics. A Decade of Transformations*. Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014. Barcelona: UOC-Huygens Editorial.

http://edcp.uoc.edu/symposia/lang/es/idp2014/proceedings/

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL