Universitat Oberta de Catalunya

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

MONOGRÁFICO

V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales

Miquel Peguera (coord.)

Sumario

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

Presentación

En el presente monográfico recogemos algunas de las intervenciones realizadas en el marco del V Congreso de Internet, Derecho y Política, que bajo el título genérico de «Cara y cruz de las redes sociales» tuvo lugar el pasado mes de julio en Barcelona.

La elección del tema del congreso no resultó difícil. En efecto, la creciente popularidad y el uso intensivo de estas redes, cuyos usuarios se cuentan por cientos de millones en todo el mundo, ponen sobre la mesa un conjunto de cuestiones de marcado interés, tanto en el plano jurídico como en el politológico. Por una parte aparecen las ventajas de estas plataformas como nuevos medios de relación social, de interacción, de intercambio de información, de generación de comunidades y superación de distancias. Pero junto a los aspectos positivos y esperanzadores, es obligado notar los riesgos que en la práctica plantean las redes sociales en relación con determinados bienes jurídicos. Algunos de los más evidentes son los que se proyectan sobre el ámbito de la intimidad o sobre el adecuado control y protección de los datos personales. Muchos usuarios deciden hacer total o parcialmente públicos algunos datos sensibles de su vida personal, renunciando aparentemente a esferas de privacidad. Esa renuncia, sin embargo, difícilmente puede haber tenido en cuenta las consecuencias que quizás a largo plazo pueden derivarse de esa despreocupada diseminación de datos privados. En la medida de lo posible, las redes sociales deben diseñarse de tal modo que contribuyan a paliar los posibles resultados negativos anticipados inadecuadamente por los usuarios. Otros problemas se suscitan en el plano de la seguridad, la suplantación de la personalidad, amenazas, *cyberbullying*, y otros ataques y conductas censurables. Es preciso valorar cómo se puede hacer frente a este tipo de riesgos, no necesariamente en términos de producción legislativa, sino de incentivo a la adopción de buenas prácticas y códigos de conducta por parte de las plataformas, y de una concienciación de los usuarios que tenga en cuenta las motivaciones efectivas que les impelen a participar de modo intensivo y no siempre suficientemente reflexivo en estas redes.

Sobre éstas y otras cuestiones se trató y se debatió a lo largo de dos días en el V Congreso IDP, en el que se abordaron también las estimulantes experiencias de participación política y ciudadana que propician las redes. El texto que reproducimos del profesor Daithí Mac Síthigh, de la Universidad de East Anglia, ofrece bajo el título genérico de «Legisladores y políticos en el punto de mira» un panorama general de los temas tratados y de las sugerencias dirigidas, tanto a los operadores jurídicos como a los políticos, en relación con el uso de las redes sociales. Daithí Mac Síthigh fue el relator del Congreso, encargado de ofrecer al final de cada jornada una síntesis comentada de los principales aspectos abordados en las ponencias y suscitados en el subsiguiente coloquio.

Además del texto del profesor Mac Síthigh recogemos en este monográfico tres de las ponencias presentadas. La primera de ellas es la intervención de Ignacio Alamillo, que se centra en cuestiones de seguridad, y de modo particular, en las políticas públicas que se están desarrollando en esta materia. Se refiere en especial a las políticas dirigidas a promover entre los usuarios la «cultura de la seguridad», concienciando a los ciudadanos sobre los riesgos y vulnerabilidades de la red y facilitando la comprensión de los elementos clave en materia de seguridad. Aborda asimismo otras políticas

públicas genéricas como las referidas al análisis y gestión de riesgos, a los sistemas de acreditación de seguridad de productos y servicios a través de mecanismos de evaluación y certificación, o a la inversión en investigación y desarrollo en materia de seguridad. Analizando el caso concreto de las políticas públicas de seguridad en Cataluña, da cuenta de las previsiones del Estatuto de Autonomía de Cataluña en este campo, así como el Plan nacional de impulso de la seguridad de las TIC adoptado por el Gobierno de la Generalitat el 17 de marzo de 2009.

Franck Durmortier, investigador del Centre de Recherches Informatique et Droit (CRID) de la Universidad de Namur, analiza las interacciones de los usuarios en las redes sociales, estudiando en particular el caso de Facebook. Examina los incentivos presentes en esta red para que los usuarios revelen información real, actualizada y completa, de donde se derivan evidentes amenazas para su privacidad. Para Durmortier, la principal de estas amenazas estriba en el riesgo de descontextualización de la información proporcionada por los usuarios. Una amenaza que se cierne no sólo sobre el derecho a la protección de los datos personales, sino que afecta también a la privacidad en un sentido más amplio, considerada como el derecho del ser humano a erigirse en sujeto múltiple y contextual, con una identidad que es configurable de modo diverso en contextos distintos. Así, defiende el autor que el derecho a la privacidad puede caracterizarse como un derecho a la integridad contextual que garantice al sujeto la posibilidad de construir su propia identidad en relaciones diferenciadas, derecho que en un entorno como Facebook se ve directamente amenazado. Durmortier propone conceptualizar el derecho a la protección de datos como una herramienta para permitir a los sujetos comportarse como *dividuos contextuales*. Plataformas como Facebook vienen en la práctica a impedir esta *dividualidad* o multi-contextualidad al facilitar la recomposición de los datos fusionando los diversos contextos en uno solo. Para contribuir a paliar este riesgo, Durmortier, en línea con las recomendaciones del Grupo de Trabajo del artículo 29 contenidas en el *Working Paper* nº 163, de 12 de junio, señala la conveniencia de que las redes sociales establezcan por defecto una configuración máximamente protectora de la privacidad, habida cuenta de que es muy bajo el porcentaje de usuarios que se preocupa por modificar la configuración establecida por defecto. Sin embargo, se muestra escéptico ante la sugerencia apuntada en dicho documento de atribuir a los usuarios, en determinados supuestos, la condición de «responsables del tratamiento», puesto que la atribución de mayor responsabilidad a los usuarios no se ajusta al nivel real de concienciación de los ciudadanos en materia de protección de datos. Las soluciones, concluye, deben venir fundamentalmente de un diseño de la arquitectura de la plataforma que permita gobernar los flujos multi-contextuales de datos en la red social.

La privacidad en las redes sociales es también el foco de la ponencia de Antoni Roig, profesor de Derecho constitucional de la Universidad Autónoma de Barcelona. El profesor Roig muestra su preocupación por los riesgos tecnológicos que amenazan la privacidad, entre otros, el peligro que supone la captura de datos que el usuario ha revelado involuntariamente, y que pueden deducirse de los perfiles de las redes sociales mediante técnicas estadísticas y heurísticas. Estos riesgos se acrecientan con la Web 3.0 y las tecnologías de web semántica. Frente a estas amenazas, las soluciones jurídicas basadas estrictamente en la protección de los datos de carácter personal resultarán a su juicio insuficientes, ya que las nuevas herramientas permitirán obtener información personal a partir de datos aparentemente inocuos muy alejados del concepto legal de dato de carácter personal. Para afrontar estos riesgos el profesor Roig apuesta por el desarrollo y la implantación de tecnologías garantes de la privacidad (*privacy enhancing technologies*, PET), buscando de este modo soluciones tecnológicas a un problema marcadamente tecnológico. Entre estas soluciones destacan las protecciones contra la explotación de datos, o *privacy-preserving data mining* (P2DM), que trata de evitar que en los análisis estadísticos se revele información personal de los usuarios. Otras tecnologías se orientan a la protección de los pseudónimos, para evitar que de los mismos pueda deducirse la identidad real del usuario, y a la vez a permitir sistemas de reputación fiables. Concluye su ponencia destacando que

la protección actual de la privacidad en las redes sociales no es hoy por hoy satisfactoria, a pesar de los esfuerzos realizados y las recomendaciones propuestas por los grupos de expertos y agencias de protección de datos. Las protecciones tecnológicas garantes de la privacidad contribuirían notablemente a aliviar los riesgos y a hacer posible un derecho efectivo a la privacidad.

Miquel Peguera Poch
Profesor de Derecho mercantil y de Derecho y nuevas tecnologías de la UOC

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

Legisladores y políticos en el punto de mira

Daithí Mac Síthigh

Fecha de presentación: agosto de 2009
Fecha de aceptación: octubre de 2009
Fecha de publicación: diciembre de 2009

Resumen
Un informe sobre el 5.º Congreso sobre Internet, Derecho y Política organizado por la UOC en julio de 2009. El autor, que participó como ponente en la conferencia y escribió un blog en vivo durante los dos días que duró el evento, examina algunas de las contribuciones, reflexiona sobre el tema de los sitios de establecimiento de redes sociales (¿a favor o en contra?) y explora los distintos enfoques de las disciplinas del derecho y las ciencias políticas, sugiriendo que el aumento de la importancia de estos sitios es un reflejo de que consideraciones como la privacidad, la seguridad, el compromiso político y los derechos de autoría son objeto de un debate público necesario e interdisciplinario.

Palabras clave
establecimiento de redes sociales, Web 2.0, gobierno abierto, derecho sobre Internet

Tema
TIC y política

Poking Lawyers and Politicians

Abstract
A report on the 5th Internet, Law and Politics conference hosted by the UOC in July 2009. The author, who attended the conference as rapporteur and wrote a 'live blog' during the two-day event, reviews some of the contributions, reflects on the theme of social networking sites ('pro or con?') and explores the different approaches of the disciplines of law and of political science, suggesting that the increased importance of such sites means that considerations such as privacy, security, political engagement and copyright are the subject of necessary and interdisciplinary public debate.

Keywords
social networking, Web 2.0, open government, Internet law

Subject
ICT and politics

1. Introducción

Los días 6 y 7 de julio de 2009 se celebró en Barcelona el 5.º Congreso anual de la UOC sobre Internet, Derecho y Política, con participantes de España, otros estados de la UE y una serie de ponentes invitados procedentes de los Estados Unidos. Las conferencias anteriores habían tratado temas como el comercio electrónico, la privacidad y el delito informático, pero la convocatoria de este año tomó como punto de partida un tema que suele arrancar los más entusiastas comentarios sobre cambios importantes en los medios, en las comunicaciones e incluso en la propia naturaleza de la amistad: los sitios de (establecimiento de) redes sociales.

La OCDE ha caracterizado el desarrollo actual de los servicios de Internet como la red participativa, extrayendo una serie de principios de la idea, a menudo amorfa, de Web 2.0 (OCDE, 2007). En el centro de este nuevo modelo de interacción facilitada por Internet se esconde la idea del sitio de establecimiento de redes sociales. Los sitios de establecimiento de redes sociales se pueden definir (Boyd y Ellison, 2007) como unidades que incluyen tres elementos, que son la construcción de un perfil de usuario (público o semipúblico, dentro de un sistema), una lista de usuarios conectados («amigos» en muchos casos), y la ulterior interconexión entre los usuarios, sus contactos y los contactos de sus contactos. Es particularmente inquietante la idea de que los sitios de establecimiento de redes sociales dan ocasión para el compromiso político, tanto si se trata del extendido deseo de lograr de nuevo el «efecto Obama» a través del uso de la tecnología para la organización política y, en último término, de la realización de campañas con éxito, incluyendo las elecciones, o simplemente para grupos, por ejemplo de estudiantes, que desean superar varias limitaciones que han evitado que protestas anteriores crecieran y se proyectaran más allá de ciertos límites (Biddix y Park, 2008).

Existe una estrecha relación entre los sitios web que centraron las discusiones de esta conferencia y otras citas académicas contemporáneas y la idea de los contenidos generados por los usuarios, con una importante representación de los usuarios jóvenes (los «nativos digitales», que han crecido en el entorno de la tecnología digital omnipresente y de la comunicación a través de medios informáticos [Palfrey y Gasser, 2008]) en ambos contextos (Green y Hannon, 2007). A través de los sitios de establecimiento de redes sociales, como Facebook y Bebo, de las plataformas de blogs, como Wordpress y Blogger y de sitios de publicación de vídeos, como Dailymotion y, por supuesto, YouTube, o incluso de sitios que combinan varios elementos, como Myspace, o nuevos elementos de microaportaciones, como el controvertido Twitter, los usuarios cuentan con nuevas oportunidades de interactuar e intercambiar materiales entre sí o, en muchos casos, con un público mucho más amplio. Los patrones históricos de actividad, por los que un número muy reducido de usuarios también contribuían con su propio contenido, parece estar cambiando; la producción de vídeos por aficionados es un elemento clave de sitios como YouTube, y en los sitios de establecimiento de redes sociales se observa un aumento en los niveles de uso y compromiso, un punto relevante para el investigador (Gauntlett, 2009).

Entender los factores de mediación social y tecnológica entre los sitios de establecimiento de redes sociales y prácticas sociales más amplias (Livingstone, 2008, pág. 396) requiere un enfoque sobrio y estricto y el papel de la ley en este aspecto sigue siendo bastante controvertido –de hecho, no es sorprendente que haya sido objeto de frecuentes escenas de «pánico moral» (Roush, 2006). Tal como Agustí Cerrillo, director del programa de Derecho y Ciencias Políticas en la UOC, indicó en la conferencia, existe un gran valor social y académico que sale a la luz en una exploración de posibles encuentros entre perspectivas distintas, aunque el centro de las preocupaciones sea Internet. Los participantes en la conferencia también usaron distintos tipos de tecnologías sociales que consideraremos en otro punto de este artículo. Durante los dos días de la conferencia, investigadores académicos, representantes electos y activistas civiles entregaron sus informes, centrados en la cuestión legal el primer día (en particular la cuestión de si las leyes actuales, nacionales o europeas, son adecuadas a este fin) y las ciencias políticas y los discursos de política el segundo.

2. Cuestiones de derecho

2.1. Salvar Facebook

Marcó la pauta James Grimmelmann, profesor adjunto de Derecho de la New York Law School y una voz importante

dentro de la comunidad académica necesariamente global de estudiantes de Ciberderecho. El estudio de Grimmelmann se basa en su propia educación como programador y jurisperito, y sus publicaciones incluyen una serie de escritos sobre el tema de los servicios web emergentes (Grimmelmann, 2004), así como los buscadores y el controvertido proyecto Google Book Search que la NYLS ha expuesto a la atención pública a través del proyecto Public Index (p. ej. Grimmelmann 2009a). Dentro de los debates sobre los sitios de redes sociales, en la conferencia y en el trabajo publicado a continuación (Grimmelmann, 2009b), argumenta que era necesario centrarse en los componentes sociales, es decir, que al considerar un tema como la privacidad, las herramientas de evaluación social (sobre todo los «atajos cognitivos» –sometidos a estudio heurístico– que se suelen usar para evaluar el riesgo) y los conceptos de daño social al menos eran tan importantes, si no más, como la atribución de problemas a determinada tecnología. Sobre esta última cuestión, Grimmelmann se basa en los esquemas taxonómicos de la privacidad de Solove (Solove, 2006), y presenta ejemplos de percepciones de libertad y privacidad, al tiempo que muestra el modo en que los sitios, en este sentido, pueden ofrecer oportunidades poco corrientes para la realización de actos hostiles o la infracción accidental de la privacidad por parte de terceros. Aunque los controles técnicos han centrado el debate público sobre el establecimiento de redes sociales y la privacidad, sigue siendo destacable que todos los usuarios –excepto una pequeña minoría– se muestran reacios a cambiar aspectos como los ajustes de privacidad controlados por los usuarios (aunque un experimento elocuente mostró que los participantes en la conferencia tendían mucho más a entender –y modificar– los ajustes de privacidad que el gran público). Un tema emergente es el de las violaciones de la privacidad por parte de semejantes (es decir, entre usuarios), lo que supone un desafío a la tradición que ve a las autoridades públicas –y, en algunos casos, a poderosos entes privados– como la principal amenaza para la privacidad individual.

2.2. ¿Qué es la privacidad?

La idea de la privacidad en sí dista mucho de ser estática y puede plantear problemas de muy diversa índole. A una escala muy básica, la noción de que la dignidad humana, un derecho fundamental de gran importancia, puede incluir ciertos aspectos que se pueden clasificar o considerar como privacidad, puede ser muy importante a la hora de perfilar los términos de la legislación y la actuación gubernamental en torno a la protección de la privacidad. Antoni Roig presentó varios puntos con relación al derecho a la dignidad, argumentando que se pueden usar las cláusulas que tratan este tema para proporcionar una actualización de las disposiciones legislativas inadecuadas, ya que la idea de la dignidad humana es más persistente y adaptable que las ideas específicas de la protección de datos, aunque las tecnologías dirigidas a mejorar la privacidad también tienen un papel muy importante que desempeñar, especialmente si se consideran antes de que la tecnología esté muy difundida. Otra perspectiva influyente y que provocó un debate entre participantes fue la de Franck Dumortier. Su análisis de la descontextualización y de Facebook trataba cuestiones que no distaban de los temas centrales del estudio de Grimmelmann, aunque el uso de enfoques teóricos sobre la privacidad y la autonomía supusieron un enlace útil entre las descripciones detalladas de los sitios de establecimiento de redes sociales y la omisión de derechos fundamentales. Dumortier delimitó las raíces de la privacidad, incluyendo las posibles tensiones entre el derecho a no ser molestado y el derecho a la integridad contextual.

Ilustrando un punto clave con un agitado debate sobre el modo en que la información sobre la propia vida sexual es muy adecuada en ciertos contextos y completamente inadecuada en otros, Dumortier adopta un enfoque escéptico sobre algunos de los alegatos de los sitios de establecimiento de redes sociales, exponiendo que el modo en que se almacena y comparte información es un desafío a la propia identidad. También emplea un argumento muy útil sobre las distinciones entre «privacidad» y «protección de datos», expresando cierta crítica sobre el lenguaje y la delimitación de este último término. No obstante, la idea de poner los derechos en práctica está íntimamente ligada al papel de la Unión Europea en materia de protección de datos, que –a pesar de que inicialmente y formalmente (de un modo controvertido), sigue anclada en el mercado interno y la armonización de las leyes nacionales a fin de evitar el proteccionismo y la distorsión del mercado– se percibe en el ámbito internacional como un alto nivel de protección de la privacidad, sin duda más completo e integrador que la mezcla de enfoques sectoriales y autorreguladores que predomina en los Estados Unidos.

Si los asistentes a la conferencia fueran miembros del Grupo sobre Protección de Datos del Artículo 29 de la

Unión, con toda seguridad habrían derramado más de una lágrima de felicidad al ver el modo en que su reciente publicación sobre el establecimiento de redes sociales en el mundo virtual (publicado en junio de 2009, unas semanas antes de la conferencia, Grupo sobre Protección de datos del Artículo 29, 2009) influía en las presentaciones e intervenciones de muchos de los participantes. El Grupo, formado como resultado de la Directiva original sobre Protección de Datos de 1995, había tenido en los últimos años un papel importante en la definición del debate a escala europea, y es conocido por su trabajo con las autoridades nacionales, el sector privado y la comunidad académica para abordar varios puntos, algunos muy controvertidos. El apoyo del Grupo a la idea de que las direcciones de IP son datos personales, por ejemplo (Grupo sobre Protección de Datos del Artículo 29, 2007), sigue contando con diversos detractores. En el caso de los sitios de redes sociales, eran muchos los que esperaban su contribución. Aunque el informe no es una fuente de derecho en sí ni una previsión exacta de ulteriores acciones legislativas, sus proposiciones –en el contexto de diversas disposiciones de derecho de la UE–, sobre los derechos de los usuarios y obligaciones de los proveedores e incluso la noción de que los usuarios sólo deberían cargar imágenes de otros una vez obtenido el consentimiento de éstos, son muy ambiciosas.

2.3. Propiedad intelectual

La cuestión de la propiedad intelectual se puede desglosar en una serie de puntos diferentes, aunque interrelacionados. Las presentaciones que se centraron con mayor detalle en temas de derecho de autoría, tanto en los Estados Unidos como en la Unión Europea, fueron las de Jane Ginsberg y Alain Strowel. En primer lugar, está el papel de los términos de uso o de los contratos de licencia de usuario final que usan con profusión los sitios populares. Aunque, en muchos casos, los usuarios no tienen acceso a asesoramiento legal independiente, o incluso apenas tienen la intención de leer o examinar los documentos que aceptan pulsando un botón mientras se registran, indudablemente son importantes fuentes de derecho y afectan al tratamiento actual y futuro del contenido cargado. Este tema gana en relevancia a medida que aumenta la cantidad de contenidos distribuidos, especialmente fotografías y material audiovisual. Por descontado, no se trata de que la concesión o cesión de derechos sea una cuestión legal o social generada por Facebook –pero el escrutinio (y posible restricción) de términos injustos sí es una preocupación creciente. Otro aspecto de los derechos de autoría y de Web 2.0 es el modo en que la idea de uso o distribución se ve afectada por nuevas formas de compartir los contenidos. Un ejemplo de ello es la definición de *intermediarios* o un subgrupo de éstos, *anfitriones*. En primera instancia, fue difícil su definición estatutaria, particularmente como se refleja en la Digital Millennium Copyright Act (DMCA) en los Estados Unidos y la Electronic Commerce Directive y la Copyright Directive en la Unión Europea, y los diversos compromisos, definiciones y amplios conceptos usados en los noventa siguen dominando el debate legal. El segundo día de la conferencia, Jordi Graells debatió sobre las licencias de Creative Commons en Cataluña. Aunque hay muchas historias positivas y ejemplos de buenas prácticas, existe un diálogo continuo entre creatividad y burocracia, y el desafío de las personas implicadas en este tipo de proyectos va más allá de entender el alcance de las leyes sobre derechos de autoría y necesita explicar la finalidad de una licencia determinada y tratar los errores de concepto y los mitos a medida que van apareciendo. Cada vez que se produzcan enfoques incoherentes de la(s) finalidad(es) de la ley sobre propiedad intelectual (fáciles de encontrar, incluso dentro de una única jurisdicción), sigue dificultándose la definición de cómo los derechos de autoría afectan a los sitios de establecimiento de redes sociales y a la amplia red de lectura-escritura. Los derechos de autoría, un ideal polifacético e intrínsecamente contradictorio, afecta a todos los participantes en la nueva web, ya sean proveedores, usuarios o autores.

3. El gobierno y la red

3.1. Ausencia de crédito

«En una era de crisis, la comunidad internacional desvía su atención hacia la sociedad de la información». Esta afirmación se recoge en la actualización del plan Avanza del Gobierno español. En esta fase de desarrollo de Internet, es común que el Gobierno asuma que la información y las tecnologías de las comunicaciones tienen un papel importante y –en opinión de algunos– determinante en el desarrollo de nuevas economías centradas en los servicios o la información. Las desventajas históricas de regiones infra-industrializadas, por ejemplo, podrían abordarse gracias a la reducción de las distancias.

Ahora, sin embargo, parece que los problemas de la actual situación económica podrían centrar el gasto público o los ahorros de costes a través de la aplicación de nuevas tecnologías. Quizá estemos más interesados en los servicios públicos y el contexto político que en atraer a las grandes industrias sólo para impulsar el desarrollo de hardware y software. La próxima Presidencia española de la UE, que comienza el 1 de enero de 2010, impulsará temas importantes como la seguridad en la red, el comercio electrónico y la protección de los derechos de autoría. Oscar Martínez, del Ministerio de Industria, explicó la relevancia de este enfoque. En cuanto al tema específico de la seguridad, el papel de la confianza, seguridad y accesibilidad nos ayuda a entender su importancia. No obstante, es importante situar este trabajo en el contexto de las recomendaciones del Consejo de Europa, la OCDE, la ITU y otras. Resumiendo, saber que existen proyectos interesantes a escala nacional puede ser una piedra angular para la cooperación internacional, aunque el entorno de seguridad seguirá en los primeros puestos de la lista de prioridades en política y defensa.

3.2. Un gobierno abierto, partidos políticos abiertos y futuras orientaciones políticas

José Manuel Alonso expuso que un gobierno abierto, en contraposición a un mero gobierno electrónico, es un objetivo que vale la pena perseguir. Sus tres pilares de servicios centrados en el ciudadano, diseñados con transparencia y responsabilidad y el impulso de la innovación, subrayan el papel de los datos accesibles en un proyecto gubernamental más amplio. Critica la atención prestada a la disponibilidad en lugar de al uso en algunos de los sistemas de medida e investigación actualmente disponibles. Por tanto, es útil el debate de Nacho Alamillo sobre riesgos en la seguridad y la necesidad de impulsar una cultura de la seguridad, al tiempo que establece un importante enlace entre la administración electrónica y la necesidad de protección y planificación adecuada. Los instrumentos legislativos europeos han tratado de impulsar una cultura de la seguridad en tres sentidos: privacidad, seguridad y administración electrónica. Teniendo en cuenta que Cataluña está desarrollando servicios electrónicos de gobierno, existe la necesidad de garantizar varias formas de protección, tanto para el sistema como para los datos.

Además de la situación económica, sin embargo, también vivimos una era en la que la confianza en los políticos está bajo mínimos, con el ejemplo de los gastos de los parlamentarios británicos citado por Ismael Peña-López durante su presentación de un panel sobre datos y gobierno. Aquí, Peña-López realizó un tributo a una herramienta desarrollada por *The Guardian* (un periódico británico) que permite a sus usuarios participar en el proyecto masivo de revisar los documentos hechos públicos; el caso, por supuesto, también ha implicado el uso de la legislación sobre libertad de información y, curiosamente, una de las propuestas presentadas por el Gobierno del Reino Unido como respuesta al comprensible enfado público fue el nombramiento de Tim Berners-Lee como asesor encargado de reformular la política de datos del Gobierno del Reino Unido. José Antonio Donaire sugiere que existe una crisis de autoridad, aunque Alberto Ortiz nos recuerda que ningún partido político puede ganar unas elecciones basándose únicamente en la promesa de digitalizar la administración. Ricard Espelt, que también participó en la conferencia, distingue entre «espacios políticos 2.0» y pura política 2.0, mostrando cómo, incluso a escala local, las preocupaciones del ciudadano pueden ser el centro de gravitación de los nuevos modelos. Su círculo virtuoso de reclamaciones, resoluciones y reformas en un análisis de la ciudad de Copons es una magnífica monografía y sirve como recordatorio de que la consideración del establecimiento de redes sociales y su contexto social no deberían tener la campaña de Obama como principio y fin. De hecho, Marta Cantijoch sugiere en su estudio que los individuos cuya orientación política se puede caracterizar como «crítica» se sienten atraídos por formas de participación poco convencionales o extrarepresentativas, y eso es algo que pueden facilitar las nuevas tecnologías. Web 2.0 puede implicar nuevos cambios, una nueva exposición a la información, más interactuación, más jóvenes, y el uso de la investigación española en la actividad política. Cantijoch expuso que ciertos usos de Internet pueden promover la participación en formas no convencionales, indicando que la distancia entre la esfera individual y la institucional se ha modificado de alguna manera.

Sin embargo, existe el riesgo de suponer que los datos o las plataformas pueden resolver todos los problemas y no someterlos a crítica. Alonso cuestionó, por ejemplo, aplicaciones como «Are You Safe Washington DC», que usa la información del catálogo de datos que el Gobierno de la

capital de EE.UU. incluye en la red como la base para una aplicación de iPhone que proporciona información sobre las estadísticas de delitos en una comunidad determinada, basándose en las herramientas de localización que incluye el dispositivo. Este uso creativo de los datos públicos también puede plantear dudas sobre las consecuencias sociales y éticas de la inclusión inmediata y visual del vecindario en una «lista negra» (imaginemos, por ejemplo, el uso de tales dispositivos por parte de los taxistas). Existe un aspecto relacionado en el poder ejercido por Apple, que mantiene un control total sobre las aplicaciones que se pueden incluir en el iTunes App Store –independientemente de si la aplicación se vende o es gratuita–, que ha demostrado ser controvertido en varias ocasiones.

4. Conclusión

4.1. Temas

Las discusiones legales centradas en el papel de la ley como facilitadora de innovación y protectora de una cultura abierta y activista. También debemos considerar si se están aplicando las leyes actuales y las consecuencias sociales de su incumplimiento, especialmente en el área de la protección de datos y la privacidad. El establecimiento de redes sociales es una parte muy importante de la vida actual, pero ciertos temas han sido objeto de una atención académica continuada (p. ej. Turkle, 1995). Las ponencias de la conferencia, especialmente las relativas a ciencias políticas, se han caracterizado por la experiencia de averiguar qué ha estado ocurriendo en la práctica, no sólo del lado de los gobiernos nacionales, sino también de entidades de menor escala y de la colaboración internacional, y a través de las acciones de usuarios que exploran los parámetros de los nuevos espacios sociales y de los medios de comunicación. Pero quedan muchas cuestiones por resolver: ¿qué haremos con estos nuevos sitios web cuando se establezcan y cómo nos mantendremos a salvo? ¿Son demasiado poderosos los sitios de redes sociales y las empresas que los respaldan? «Esperar a ver» ha sido una constante en conferencias anteriores en otros lugares, pero los debates celebrados el pasado julio en Barcelona sugieren que se ha llegado al momento en que habrá una intervención legislativa en un futuro no muy lejano o bien se considerará completamente indeseable o inadecuada para un futuro previsible.

4.2. Tecnologías

Conviene hacer un comentario final sobre el uso de los medios de comunicación social y las diversas tecnologías por parte de los participantes en la conferencia. Usando la etiqueta «idp2009», fue sencillo para los participantes y el público a distancia llevar un seguimiento del contenido de una serie de autores y en diferentes medios. El autor de esta nota tenía un papel oficial en el evento como «informador», pero su papel no era simplemente presentar un informe al final del día al estilo tradicional, sino escribir un blog en vivo de cada sesión, tomando notas con un ordenador portátil y publicando un resumen de cada sesión en cuanto terminaba o poco después. Esta práctica es de cierta utilidad para el gran público que desea elaborar un estudio académico, y puede contribuir al impacto del estudio de una nación a través de una difusión rápida y económica, pero también supone un cambio en la forma en que se desarrolla una conferencia académica y puede aportar sus propios desafíos en términos de expectativas de inmediatez y del tipo de presentaciones que se realizan.

De hecho, todo lo aquí comentado subraya la importancia del investigador, no como un seguidor entusiasta de cada nuevo servicio, sino como observador y participante crítico y comprometido. Con la experiencia de muchos asistentes en el uso de los sitios de establecimiento de redes sociales, así como con las dimensiones de investigación y reguladoras con las que otros están familiarizados, existe una gran responsabilidad para que cada persona presente los problemas, las posibles lagunas en los sistemas legales o políticos y las implicaciones a largo plazo. Además, si consideramos conferencias anteriores, los sitios que se han puesto a debate serán diferentes –con mayor presencia de Myspace y menor de Twitter. Este ultimo servicio es particularmente importante; algunos de los debates y comentarios más vibrantes se difundieron a través de esta controvertida plataforma en inglés, español y catalán (nótese que las presentaciones reales fueron en los tres idiomas, usando traducción simultánea *in situ* del modo convencional, con intérpretes profesionales y un sistema inalámbrico de sonido). Los desafíos políticos, sociales y legales que suponen servicios emergentes como Twitter serán, con toda probabilidad, objeto de investigaciones futuras y quizá de futuras conferencias dentro de esta serie.

Bibliografía

ARTICLE 29 WORKING PARTY (2007). *Opinion 4/2007 on the concept of personal data*. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf>

ARTICLE 29 WORKING PARTY (2009). *Opinion 5/2009 on online social networking*. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf>

BIDDIX, J.; PARK, H. (2008). «Online networks of student protest: the case of the living wage campaign». *New Media and Society*. Vol. 10, pág. 871-891.

BOYD, D.; ELLISON, N.B. (2007). «Social network sites: definition, history, and scholarship». *Journal of Computer-Mediated Communication*. Vol. 13, n.º 1, art. 11. [Fecha de consulta: 26/10/09]. <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>

GAUNTLETT, D. (2009). «Media studies 2.0». *Interactions*. Vol. 1, pág. 147-158.

GREEN, H.; HANNON, C. (2007). *Their space: education for a digital generation*. Londres: Demos. 84 pág.

GRIMMELMANN, J. (2004). «Virtual Worlds as Comparative Law». *New York Law School Law Review*. Vol. 49, pág. 147-184.

GRIMMELMANN, J. (2009a). «How to Fix the Google Book Search Settlement». *Journal of Internet Law*. Vol. 12, n.º 10, pág. 10-20.

GRIMMELMANN, J. (2009b). «Saving Facebook». *Iowa Law Review*. Vol. 94, pág. 1137-1206.

LIVINGSTONE, S. (2008). «Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression». *New Media and Society*. Vol. 10, pág. 393-411.

OECD (2007). «Participative Web: User-Created Content» (DSTI/ICCP/IE(2006)7).

PALFREY, J.; GASSER, U. (2008). *Born digital: understanding the first generation of digital natives*. New York: Basic Books. 375 pág.

ROUSH, W. (2007). «The moral panic over social-networking sites» [artículo en línea]. *Technology Review*. [Fecha de consulta: 26/10/09]. <http://www.technologyreview.com/communications/17266/>

SOLOVE, D. (2006). «A Taxonomy of Privacy». *University of Pennsylvania Law Review*. Vol. 154, pág. 477-560.

TURKLE, S. (1995). *Life on the screen: identity in the age of the Internet*. Nueva York: Simon & Schuster. 347 pág.

Cita recomendada

MAC SÍTHIGH, Daithí (2009). «Legisladores y políticos en el punto de mira». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_mac-sithigh/n9_mac-sithigh_esp>

ISSN 1699-8154

Sobre el autor

Daithí Mac Síthigh
d.mac-sithigh@uea.ac.uk

Daithí Mac Síthigh es profesor en la Facultad de Derecho de Norwich, University of East Anglia, y centra su interés como docente e investigador en el derecho y la regulación de Internet, en el derecho comparado de medios de comunicación, derecho constitucional y administrativo y propiedad intelectual. En el 2009, finalizó la tesis para su doctorado de Filosofía sobre la aplicación del derecho de los medios de comunicación a Internet y asistió como informador a la conferencia de la UOC, publicando actualizaciones sobre ésta en su blog académico Lex Ferenda.

University of East Anglia
Room 205, second Floor, Earlham Hall
Norwich, NR4 7TJ, Reino Unido

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

Las políticas públicas en materia de seguridad en la sociedad de la información

Ignacio Alamillo

Fecha de presentación: septiembre de 2009
Fecha de aceptación: noviembre de 2009
Fecha de publicación: diciembre de 2009

Resumen
La mayoría de los Estados se encuentran en el proceso de establecer una aproximación basada en múltiples participantes -aparte de los propios gobiernos- y una estructura de gobernanza de alto nivel para la implementación de políticas de alcance nacional.
En este sentido, estos Estados han hecho avances importantes en el desarrollo de marcos nacionales de políticas de seguridad, han aprobado medidas para combatir el cibercrimen y han establecido equipos de respuesta a incidencias de seguridad informática. Este artículo presenta las principales políticas y actuaciones públicas para la promoción de la seguridad de la información, y se centra específicamente en las actuaciones realizadas en Cataluña y en el Estado español en esta materia.

Palabras clave
políticas públicas de seguridad, cibercrimen, seguridad de la información

Tema
Protección de datos

Public Security Policies in the Information Society

Abstract
Most countries are in the process of reaching agreement among multiple participants - apart from the governments themselves - establishing a high level management structure for the implementation of national policies. Major advances have been made in the development of national frameworks for security policies, measures for combating cybercrime have been approved, and response teams for security issues have been established. This article presents the main public policies and legal proceedings for promoting information security, focussing specifically on legal proceedings which have been carried out in Catalonia and the rest of Spain.

Keywords
public security policies, cybercrime, information security

Subject
Data protection

1. Las políticas públicas de impulso genérico de la seguridad de la información

En esta sección presentamos las políticas públicas de seguridad de la información, desde una perspectiva genérica, común a toda la problemática de la seguridad de la información.

1.1. Estrategia global de seguridad de la información

El desarrollo de una estrategia global de seguridad de la información a nivel nacional empieza a ser una constante entre los Estados, una política habitualmente centrada en la necesidad de desarrollar herramientas de investigación y de concienciación del público en cuanto al número cada vez más importante de amenazas y vulnerabilidades de la seguridad en línea.

En algunos casos, se han desarrollado políticas nacionales para coordinar actuaciones previas individuales que perseguían objetivos muy concretos tratando de crear una política o estrategia global de seguridad, mientras que en otros casos las políticas nacionales se han dirigido a la implementación de políticas de administración electrónica e incluso de iniciativas singulares, como las firmas electrónicas o las tarjetas de ciudadanos.

La mayoría de los Estados se encuentran en fase de establecer algún tipo de estrategia global de la seguridad de la información, con dos rasgos característicos:

- Una aproximación multidisciplinar y con múltiples participantes.
- Una estructura de gobernanza de alto nivel.

Con respecto a la aproximación multidisciplinar y con múltiples participantes de las políticas nacionales de seguridad de la información, resulta interesante que la mayoría de las iniciativas constatan que la cultura de la seguridad no aparece sencillamente a partir de las soluciones tecnológicas.

Al contrario, se necesita una aproximación más amplia, que tome en consideración también los aspectos socioeconómicos y legales, lo que imprime una dimensión multidisciplinar a las políticas.

Además, se considera que los gobiernos, por sí solos, no pueden gestionar todos los retos y cuestiones de seguridad, lo que implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes.

Resulta también frecuente que los gobiernos acudan al sector privado para recibir asesoría sobre desarrollos tecnológicos y de implementación global. Algunos Estados contratan a universidades y a expertos independientes para proporcionar ayuda en cuestiones de política, o crean la justificación necesaria para la implementación de una política concreta.

Como cuestión pendiente en la mayoría de los Estados, podemos encontrar la limitada participación de la sociedad civil en las cuestiones de seguridad de la información, lo que indica la necesidad de mejorar dicha participación.

Por lo que respecta a la estructura de gobernanza, la mayoría de los Estados posiciona su estructura de gobernanza de la seguridad al más alto nivel. En muchas ocasiones, encontramos una dependencia de esta estructura de seguridad de la oficina del Gobierno o del primer ministro y, de manera más escasa, como parece ser el caso del Estado español, esta responsabilidad se encuentra repartida entre diferentes departamentos ministeriales.

En todos los casos, es preciso indicar que una aproximación jerárquica, de arriba abajo, no resulta suficiente, también es necesaria la cooperación próxima de la industria y de todos los actores de la sociedad de la información, con el Gobierno como coordinador de los esfuerzos y actividades requeridas.

Más allá de las fronteras nacionales, se necesita la colaboración con las organizaciones internacionales y el resto de gobiernos para conseguir el objetivo de la seguridad, ya que la actividad individual de los Estados no puede dar respuesta al reto global de la seguridad de Internet, que no conoce fronteras.

En el Estado español, el Plan Avanza, liderado por el Ministerio de Industria, Turismo y Comercio, mediante la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, ha sido uno de los instrumentos importantes en relación con la estrategia global española de

seguridad de la información, de la que ha surgido una línea relevante de servicios a los ciudadanos y a las empresas, ofrecidos por el INTECO.

También es preciso referirse a la actuación del Centro Nacional de Inteligencia/Centro Criptológico Nacional, dependiente del Ministerio de Defensa, en relación con la política de seguridad de información clasificada en el ámbito de la defensa y la seguridad nacional, que incluye la participación en la OTAN, y la operación del Esquema nacional de evaluación y certificación de la seguridad de la información, orientado a la seguridad de los productos, tanto de ámbito militar como civil, y que se presenta posteriormente.

Finalmente, en el ámbito catalán, es necesario referirse al Plan nacional de seguridad de la información de Cataluña, aprobado por acuerdo del Gobierno de la Generalitat de Cataluña de 17 de marzo del 2009.

1.2. Concienciación y formación sobre la seguridad de la información

Una de las políticas públicas genéricas más importante es aquella que se orienta a incrementar los niveles de conciencia sobre la necesidad de la seguridad de la información, que la OCDE denomina la «cultura de la seguridad».

A este aspecto se han dedicado las importantes Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de la seguridad, del año 2002, que sustituyen a las directrices de seguridad de los sistemas de información del año 1992.

Las directrices parten de la noción de un importante cambio en la computación, que ha pasado de sistemas aislados y redes privadas a un entorno basado en ordenadores personales, tecnologías convergentes, el uso masivo de redes públicas como Internet y la interconexión de sistemas abiertos. En este nuevo contexto, Internet se ha convertido en parte de las infraestructuras operativas de sectores estratégicos como la energía, los transportes y las finanzas, y se encuentra en la base del comercio y el gobierno electrónicos, además de permitir nuevas posibilidades a los ciudadanos.

Como contrapartida, han surgido nuevas vulnerabilidades y amenazas a la seguridad de la información y las comunicaciones, que es preciso tratar adecuadamente, comenzando por un nivel suficiente de conocimiento de los nuevos retos de seguridad, para llegar a una cultura de la seguridad que abarque a todos los participantes en la sociedad de la información.

Los propósitos de las directrices son los siguientes:

- Promover una cultura de seguridad entre todos los participantes como medio para proteger los sistemas y redes de información.
- Incrementar la concienciación sobre el riesgo de los sistemas y redes de información sobre las políticas, prácticas, medidas y procedimientos disponibles para poder hacer frente a estos riesgos, así como sobre la necesidad de adoptarlos y ejecutarlos.
- Motivar entre todos los participantes una mayor confianza en los sistemas y redes de información, así como en su forma de operación y de uso.
- Crear un marco general de referencia que ayude a los participantes en la comprensión de los aspectos de seguridad y con respecto a los valores éticos en el desarrollo y la ejecución de políticas coherentes, así como de prácticas, medidas y procedimientos para la seguridad de sistemas y redes de información.
- Suscitar entre todos los participantes, cuando sea posible, la cooperación y el intercambio de información sobre el desarrollo y la ejecución de políticas de seguridad, así como de prácticas, medidas y procedimientos.
- Promover el conocimiento en materia de seguridad como un objetivo importante que se debe alcanzar entre todos los participantes involucrados en el desarrollo y la ejecución de normas técnicas.

En el marco de estos objetivos generales, se proponen nueve principios, complementarios entre sí, de interés político y técnico, con indicación expresa de que los esfuerzos por fortalecer la seguridad de los sistemas y redes de información deben respetar los valores democráticos y, en particular, garantizar tanto flujos de comunicación libres y abiertos como la protección de los datos de carácter personal:

1. Concienciación. Los participantes deben ser conscientes de la necesidad de disponer de sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

2. Responsabilidad. Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

3. Respuesta. Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten a la seguridad.

4. Ética. Los participantes deben respetar los intereses legítimos de terceros.

5. Democracia. La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6. Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

7. Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

8. Gestión de la seguridad. Los participantes deben adoptar una visión integral de la administración de la seguridad.

9. Evaluación continua. Los participantes deben revisar y evaluar periódicamente la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Continuando con su actividad de promoción de la cultura de la seguridad, la OCDE preparó en el año 2003 un plan de implementación que identifica aspectos importantes con respecto a los diferentes roles o funciones de los participantes, sobre la base de la necesidad de una cooperación continuada entre los gobiernos, las empresas y la sociedad civil.

En opinión de la OCDE, los gobiernos tienen la responsabilidad de emprender el liderazgo del desarrollo de la cultura de la seguridad, mediante las diferentes funciones que cumple en relación con los sistemas y redes de la información (desarrollador de políticas públicas, propietario y operador de sistemas y redes).

Durante el proceso de desarrollo de políticas públicas, los gobiernos deben promover la seguridad de las redes y los sistemas de información para generar confianza en su uso y asegurar mejor la seguridad global. A pesar de ser un proceso propio, los gobiernos deberían desarrollar estas políticas públicas de manera transparente, mediante consultas con otros gobiernos y con otros interesados.

Los gobiernos también deben desarrollar políticas públicas nacionales o regionales sobre seguridad de la información y certificar la cooperación internacional para promover esta cultura global de la seguridad mediante instrumentos como los siguientes:

- Medidas legales y técnicas para combatir la ciberdelincuencia, coincidentes con la Convención del Consejo de Europa, que presentaremos posteriormente.
- Equipos y recursos personales altamente cualificados para proporcionar soporte a la lucha coordinada contra el fraude informático.
- Instituciones preparadas para responder a ataques y emergencias informáticas, así como para intercambiar información al respecto, por ejemplo, los denominados CERT.
- Mecanismos de cooperación con el sector privado para combatir con mayor efectividad los problemas de seguridad.
- Apoyo a la investigación y el desarrollo en el campo de la seguridad de las tecnologías de la información.
- Actividades de concienciación pública, de formación y educación del público.
- Suministro de recursos de información al público sobre la seguridad de los sistemas y redes de información.

Como propietarios y operadores de sistemas y redes de información, los gobiernos comparten papel con las empresas, otras organizaciones y los individuos en cuanto a asegurar el uso correcto de los sistemas y las redes, dentro de la cultura de la seguridad.

En general, debido al volumen de los sistemas de los gobiernos en relación con el territorio nacional, éstos deberían ser un modelo y ejemplo de operación segura, para guiar al resto de organizaciones y ciudadanos mediante el establecimiento de mejores prácticas y otras técnicas de mejora organizativa; mientras que, en particular, es necesario considerar la capacidad de adquisición de tecnología que tienen los gobiernos como un mecanismo para influir en la mejora de la seguridad de los productos ofrecidos en el mercado.

El análisis realizado por la OCDE a finales del 2004 sobre las actividades gubernamentales, en relación con la seguridad de la información y, en particular, sobre el marco normativo en apoyo de la seguridad, ha mostrado que una serie importante de Estados identifican la firma electrónica y la certificación digital como aspecto esencial de su estrategia legal en apoyo de la seguridad.

Adicionalmente, se identifican como elementos importantes la protección de datos personales y las medidas de inspección y control sobre las comunicaciones electrónicas.

Con respecto a los programas de sensibilización sobre la seguridad de la información, ENISA ha publicado un interesante documento, dirigido a ayudar a los Estados miembros de la Unión a preparar este tipo de programa, en el que expone sus beneficios principales:

1. Representar un punto de referencia y un motor para una serie de actividades de sensibilización, formación y educación relacionadas con la seguridad de la información, de las que ya existen algunas, pero que posiblemente deban ser objeto de una mayor coordinación y optimización.

2. Transmitir las directrices o prácticas recomendadas importantes que sean necesarias para proteger los recursos de información.

3. Facilitar información general y específica sobre los riesgos y controles de la seguridad de la información a las personas que deban conocerla.

4. Informar a las personas de sus responsabilidades en relación con la seguridad de la información.

5. Estimular a las personas a adoptar las directrices o prácticas recomendadas.

6. Crear una cultura de seguridad más arraigada, con una comprensión y un compromiso de amplio alcance respecto a la seguridad de la información.

7. Contribuir a potenciar la coherencia y eficacia de los controles de la seguridad de la información y fomentar la adopción de controles efectivos con respecto a su coste.

8. Favorecer la reducción del número y el alcance de las infracciones de la seguridad, para disminuir así el coste directamente (por ejemplo, daños producidos por virus) e indirectamente (por ejemplo, reducción de la necesidad de investigar y solucionar las infracciones). Éstas son las principales ventajas financieras del programa.

Los últimos estudios muestran que los Estados ya se encuentran activamente involucrados en iniciativas para incrementar la concienciación pública en relación con la cultura de la seguridad, iniciativas que incluyen presentaciones públicas y la distribución de materiales informativos.

Por ejemplo, en el Estado español se pueden mencionar varias iniciativas en este sentido, que incluyen el proyecto de divulgación del estado de la seguridad FARO, de ASIMELEC; el *road-show* EXPOSEC para presentar aspectos de seguridad, también realizado por ASIMELEC en colaboración con el Ministerio de Industria, Turismo y Comercio; la constante tarea divulgadora de las cámaras de comercio, en particular de Camerfirma; o la actuación de la sociedad civil, por ejemplo, mediante el Foro de las evidencias electrónicas, que genera discusión en línea y reuniones periódicas con todos los actores en torno a aspectos relativos a la seguridad de la información, como la generación de pruebas electrónicas con reconocimiento judicial.

Los actos públicos tratan una importante variedad de temas de seguridad, cuestiones muy generales o más específicas como la gestión de riesgo, la autenticación electrónica, las firmas electrónicas o las infraestructuras de clave pública (PKI). El público destinatario de estos acontecimientos también resulta variable, desde el público en general hasta expertos que trabajan en el sector privado y el sector público. En particular, muchos gobiernos llevan a cabo de manera regular actuaciones internas para formar a su personal (por ejemplo, el Centro Criptológico Nacional tiene una importante actividad en éste sentido), con una incipiente tendencia a abrir estos actos al sector privado y a los ciudadanos, que puede ser un modo más efectivo de llegar a estos destinatarios.

Por otra parte, la preparación y distribución gratuita de recomendaciones, mejores prácticas y guías generales es una manera muy importante de vehicular las políticas de concienciación de la seguridad.

Además, en varios Estados existe la tendencia a redactar mejores prácticas y guías en cuestiones técnicas y operativas, como la autenticación en línea, las firmas electrónicas, las redes sin hilos, las redes entre iguales (*peer-to-peer*), la gestión del riesgo y la respuesta a incidentes.

1.3. Análisis y gestión de riesgo

El análisis y la gestión de riesgo es también una política genérica importante en varios Estados, entre los que se incluye el español.

Las iniciativas relacionadas con el análisis y la gestión de riesgo incluyen casos como el desarrollo de metodologías (Francia, con EBIOS, o España, con MAGERIT), o normas y guías (Noruega, Japón o EE. UU.). Algunas iniciativas se completan con una red específica de usuarios, como sucede en Francia, para el intercambio de información y para continuar el desarrollo de la metodología.

Otras iniciativas incluyen la creación y el suministro de herramientas automáticas para asistir en la realización de los análisis de riesgo, como es el caso de la herramienta PILAR del Centro Criptológico Nacional o de las herramientas del método CRAMM británico.

Es preciso indicar que el uso de las técnicas y herramientas de análisis y gestión de riesgo no se encuentra limitado a las tecnologías de la información, sino que también se empieza a utilizar en áreas como las de los desastres naturales o el sector de las telecomunicaciones y, de manera más genérica, para la protección de las infraestructuras críticas.

Asimismo, en algunos Estados, como Austria, el análisis de riesgo forma parte de los procesos de supervisión y control de los prestadores de servicios de certificación de firma electrónica, mientras que en Finlandia se ha utilizado como herramienta para los proyectos de cooperación financiera liderados por el Gobierno.

1.4. Evaluación de la seguridad de la información en productos y servicios

Con una orientación más particular hacia los productos, se encuentra ya consolidada la política de los Estados de fomentar la calidad y la seguridad de aquéllos mediante su certificación conforme a metodologías formales. Cada vez son más los Estados que exigen certificaciones de seguridad en los productos que han de adquirir para la realización de sus tareas.

El modo de implementar esta evaluación y certificación de la seguridad de la información consiste en la creación de un esquema nacional de evaluación, que permite la organización sistemática de las funciones de evaluación y certificación de la seguridad dentro de un país concreto, bajo la autoridad de un consejo de dirección o de una entidad de certificación de la seguridad, y tenga como objeto confirmar que se mantienen unos altos niveles de competencia y de imparcialidad, así como la consecución de la coherencia global del sistema.

Los esquemas nacionales se crean al amparo del Acuerdo de reconocimiento mutuo sobre los certificados de evaluación de la seguridad de las tecnologías de la información, de 26 de noviembre de 1997, aprobado por el grupo de altos funcionarios en seguridad de los sistemas de información de la Comisión Europea, de acuerdo con el mandato contenido en el punto tercero de la Recomendación del Consejo 95/144/CE, de 7 de abril de 1995.

Centrados inicialmente en la certificación de producto, de acuerdo con los criterios de evaluación de la seguridad de las tecnologías de la información (ITSEC) de 1991, en la actualidad, los Estados signatarios del Acuerdo también han asumido los llamados criterios comunes para la evaluación de la seguridad de las tecnologías de la información (*Common Criteria* o CC, ISO 15408), mediante la modificación del Acuerdo de 1997, así como la firma del Acuerdo sobre el reconocimiento de los certificados de criterios comunes en el campo de la seguridad de la tecnología de la información, de 23 de mayo del 2000.

Un esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información funciona de la manera siguiente:

- El esquema nacional es dirigido por un único organismo de certificación, de acuerdo con una política establecida por el propio organismo de certificación o por un consejo de dirección del esquema nacional, que deben crear y hacer cumplir los reglamentos operativos de aquél.
- El organismo de certificación ha de ser un organismo independiente, declarado competente por una norma legal o administrativa, o bien acreditado por una entidad de acreditación nacional. En cualquier caso, debe cumplir los requisitos EN 45011 o Guía ISO 65, o los requisitos descritos en el anexo C del Acuerdo ITSEC.
- El organismo autoriza la participación de los servicios de evaluación del esquema, controla el funcionamiento y la actividad de evaluación, examina todos los informes de ésta, elabora un informe de certificación con respecto a cada una de ellas y publica los certificados y los informes de certificación, así como una lista de productos certificados.

- El servicio o laboratorio de evaluación, además de ser autorizado por el organismo de certificación, debe ser previamente certificado por una entidad de acreditación nacional, excepto si ha sido creado y declarado competente por una norma legal o administrativa. En cualquier caso, ha de cumplir los requisitos EN 45001 o Guía ISO 25.

El Centro Criptológico Nacional, creado por el Real Decreto 421/2004, ha sido denominado órgano competente de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información, mientras que el Instituto Nacional de Técnica Aeroespacial (INTA) actúa como laboratorio de evaluación autorizado para productos que traten información clasificada y no clasificada, y la empresa APPLUS actúa como laboratorio de evaluación autorizado para productos que traten información no clasificada, y ENAC como entidad de acreditación.

1.5. Investigación y desarrollo en seguridad de la información

La investigación y el desarrollo en materia de seguridad de la información es una de las políticas más habituales de los Estados avanzados en la cultura de la seguridad, especialmente por el impacto posterior en la competitividad de las empresas productoras de tecnologías de seguridad, que comercializan sus productos en el mercado global.

En este sentido, desde una perspectiva de política de la Unión Europea, la Resolución del Consejo, de 22 de marzo del 2007, sobre una estrategia para una sociedad de la información segura en Europa, considera que los recursos destinados a investigación y desarrollo (I+D) e innovación, tanto a nivel nacional como comunitario, constituyen uno de los elementos fundamentales para reforzar el nivel de seguridad de las redes y de la información de los nuevos sistemas, aplicaciones y servicios.

En consecuencia, se considera importante intensificar el esfuerzo a escala europea en los ámbitos de la investigación y la innovación en relación con la seguridad, en particular mediante el Séptimo programa marco y el Programa marco para la competitividad y la innovación.

Adicionalmente, es preciso realizar esfuerzos para implantar medidas destinadas a la difusión y promoción de la explotación comercial de los resultados, incluida la evaluación de su utilidad para la comunidad en su conjunto, lo que contribuirá a mejorar la capacidad de los proveedores europeos para suministrar soluciones de seguridad que respondan a las necesidades específicas del mercado europeo.

La mayoría de los Estados reconocen la importancia de las actividades de investigación y desarrollo para la seguridad de la información, ya que son la clave para producir soluciones innovadoras que puedan hacer frente a los requisitos presentes y futuros de la seguridad de la información. Como se ha avanzado, la inversión en investigación y desarrollo en seguridad de la información se percibe como un elemento que contribuye al incremento global de innovación y competitividad de los Estados.

Sin embargo, los estudios muestran que pocos Estados han establecido programas específicos de investigación en seguridad de la información con fondos públicos; la mayoría financia la investigación en seguridad mediante programas más amplios de investigación, habitualmente relativos a los aspectos computacionales (por ejemplo, criptografía) y tecnológicos, sin que se consideren de modo general los aspectos sociales, legales y económicos de la seguridad de la información.

De manera general, estas tareas de investigación y desarrollo son realizadas por las universidades, habitualmente por institutos específicamente creados para tratar la cuestión de la seguridad de la información y, con menos frecuencia, en cooperación con la industria. También resulta notable que la cooperación internacional en materia de investigación y desarrollo de la seguridad de la información sea limitada.

Como ejemplos de las actividades en esta área, se pueden mencionar los siguientes:

- El proyecto de los Países Bajos SENTINEL, con el objetivo de desarrollar aplicaciones seguras para sistemas de usuario, administración electrónica y comercio electrónico, que presenta una interesante aproximación multidisciplinar.
- El proyecto Oppidum (Francia) y el IKT SoS (Noruega).
- Los proyectos Seguridad 2020 (España) y los proyectos españoles de investigación específica, dentro de líneas de alcance tecnológico más amplio (caso similar

a Austria, Dinamarca, Alemania, Corea, Reino Unido o EE. UU.).

En algunos casos, las tareas de investigación son apoyadas o realizadas por organizaciones gubernamentales con responsabilidades de seguridad de la información, como la Oficina federal alemana de seguridad de la información, la Agencia coreana de seguridad de la información, el Establecimiento público canadiense de seguridad de las comunicaciones o la División de ciberseguridad del Departamento de Interior de Estados Unidos. Estas tareas de investigación persiguen el desarrollo de nuevas soluciones, como RFID, biometría o tecnología sin hilos, o solucionar necesidades o problemas inmediatos.

En otros casos, los Estados facilitan la participación de la industria y de otras instituciones independientes de investigación en sus iniciativas de búsqueda de seguridad de la información, como es el caso de España, Alemania, los Países Bajos o Austria.

2. El Plan nacional de seguridad de la información de Cataluña

El 17 de marzo del 2009, por Acuerdo de Gobierno 50/2009, publicado en el DOGC 5351, de 1 de abril, se aprobó el Plan nacional de seguridad de la información de Cataluña, según las competencias de la Generalitat de Cataluña en sociedad de la información y, en concreto, en el acceso a las tecnologías de la información y la comunicación (TIC), en comercio electrónico y consumo, y en administración electrónica, por el que se cree, en su caso, un centro de seguridad de la información de Cataluña (CESICAT), a fin de que desarrolle los objetivos estratégicos del Plan.

2.1. La seguridad TIC en el Estatuto de autonomía de Cataluña del 2006 (EAC)

Uno de los fundamentos importantes para afirmar la competencia de la Generalitat de Cataluña, y del resto de administraciones públicas catalanas en seguridad de la información, procede del importante artículo 40 del EAC («protección de las personas y de las familias»).

En este sentido, debemos partir del artículo 40.1, que exige a los poderes públicos «tener como objetivo la mejora de la calidad de vida de todas las personas» que, evidentemente, es necesario considerar aplicable en el más amplio sentido y, por supuesto, a la sociedad de la información, en la que las personas desarrollan una parte cada vez más importante de su vida.

Con respecto a los colectivos que se deben proteger especialmente, el artículo 40.3 del EAC determina que «los poderes públicos deben garantizar la protección de los niños, especialmente contra toda forma de explotación», incluyendo las formas de explotación que se pueden producir utilizando medios electrónicos, como en casos de acoso a través de la Red (*ciberbullying*) o de acoso sexual; una previsión estatutaria que se debe poner en relación con el artículo 142, que establece las competencias de la Generalitat en materia de juventud.

Asimismo, el artículo 40.6 del EAC establece que «los poderes públicos deben garantizar la protección de las personas mayores para que puedan llevar una vida digna e independiente y participar en la vida social y cultural», mandamiento estatutario que exige dirigir de manera específica los riesgos que la gente mayor puede sufrir en las redes telemáticas, para favorecer su integración y participación efectiva en la sociedad de la información, que dependerá, en parte, del grado de confianza que aquélla posea.

Finalmente, el artículo 40.8 del EAC indica que «los poderes públicos deben promover la igualdad de todas las personas con independencia del origen, la nacionalidad, el sexo, la raza, la religión, la condición social o la orientación sexual, y también deben promover la erradicación del racismo, del antisemitismo, de la xenofobia, de la homofobia y de cualquier otra expresión que atente contra la igualdad y la dignidad de las personas», obligación estatutaria que también hay que cumplir en relación con las nuevas formas de discriminación y todas las formas de atentados a los derechos y libertad que se puedan producir utilizando medios electrónicos, entre los que se incluyen los ciberdelitos.

Por su parte, el artículo 42.3 del EAC («cohesión y bienestar sociales») insiste en la obligación de los poderes públicos de «velar por la dignidad, la seguridad y la protección integral de las personas, especialmente de las más vulnerables», mención expresa de la seguridad que se debe considerar aplicable de manera plena a la seguridad de la sociedad de la información catalana.

Otro fundamento importante en relación con la competencia para actuar en esta materia lo encontramos en el artículo 49.1 del EAC («Protección de los consumidores y usuarios»), cuando determina que «los poderes públicos deben garantizar la protección de la salud, la seguridad y la defensa de los derechos y los intereses legítimos de los consumidores y usuarios».

Contiene esta norma otra referencia expresa a la seguridad, que también debe entenderse plenamente aplicable a la seguridad en la Red, en este caso con una especial atención a los consumidores y los usuarios (una parte muy importante de la ciudadanía, en el modelo económico actual), y que se identifica con un colectivo que debe ser protegido de modo específico.

Precisamente en relación con este colectivo se libra en la actualidad una de las batallas importantes contra el fraude, en concreto frente al robo de identidades financieras (mediante el *phishing*), el robo de informaciones comerciales sensibles, como los datos de las tarjetas de pago, o contra las comunicaciones comerciales no solicitadas (*spam*).

Es preciso señalar que el artículo 123 del EAC determina la competencia exclusiva de la Generalitat de Cataluña en materia de consumo, indicando los aspectos de formación y educación, que resultan particularmente importantes en materia de seguridad de las TIC.

Con respecto al comercio electrónico, también hay que señalar la competencia exclusiva de la Generalitat de Cataluña relativa a su ordenamiento administrativo, según el artículo 112.1.a) del EAC, lo que, de acuerdo con la nueva ley de impulso de la sociedad de la información, incluye la declaración de las medidas de seguridad aplicables al comercio electrónico.

Más concretamente, el artículo 53 del EAC («Acceso a las tecnologías de la información y de la comunicación») impone obligaciones de actuación positiva a los poderes públicos en relación con las TIC, y en concreto, su apartado 1 determina que «los poderes públicos deben facilitar el conocimiento de la sociedad de la información y deben impulsar el acceso a la comunicación y a las tecnologías de la información, en condiciones de igualdad, en todos los ámbitos de la vida social, incluido el laboral; deben fomentar que estas tecnologías se pongan al servicio de las personas y no afecten negativamente a sus derechos, y deben garantizar la prestación de servicios por medio de dichas tecnologías, de acuerdo con los principios de universalidad, continuidad y actualización».

Como resulta evidente en el texto, la actuación pública debe garantizar que las tecnologías no afecten negativamente a los derechos de las personas, lo que exige de un programa público de seguridad de la sociedad de la información que se responsabilice de ello.

Por otra parte, el principio de continuidad impuesto por el EAC obliga a la vigilancia y protección de los elementos que componen la infraestructura crítica de las TIC, tanto cuando ésta se encuentra bajo responsabilidad de las administraciones y, en general, del sector público como en manos del sector privado, con el que es necesario establecer políticas de colaboración y apoyo mutuo.

Otra dimensión de actuación en materia de seguridad de las TIC deriva, por conexión, del resto de competencias de la Generalitat de Cataluña y de los gobiernos locales de Cataluña. Este es el caso, en relación con las competencias de seguridad y protección civil (artículo 132 del EAC), de seguridad pública (artículo 164 del EAC) y privada (artículo 163) o energía y, en concreto, en materia de seguridad nuclear, ya que los efectos de un incidente de seguridad de la información pueden manifestarse civilmente, lo que produce un efecto en cascada, especialmente cuando los incidentes afectan a las infraestructuras críticas TIC, que dan soporte a los sectores gubernamental y productivo que dependen de éstas.

Esta competencia en materia de seguridad TIC sobre infraestructuras críticas se fundamenta, adicionalmente, en el artículo 140.7 del EAC, en relación con las redes de comunicaciones electrónicas, cuya seguridad es necesario proteger, ya que estas redes son el factor principal que permite la existencia y la continuidad de la sociedad de la información. Como hemos visto anteriormente, la política de la Unión Europea en materia de seguridad TIC se trata en la sede del marco reglamentario de las comunicaciones electrónicas, en que el EAC otorga competencias ejecutivas a la Generalitat de Cataluña.

Finalmente, corresponde a la administración pública la competencia de organización y regulación del funcionamiento administrativo propio, así como el régimen jurídico

y procedimiento administrativo (artículo 159 del EAC), en el contexto de la legislación estatal básica, y en materia TIC, dentro del marco de la ley de acceso electrónico de los ciudadanos a los servicios públicos, que trata extensamente las obligaciones de seguridad de la actuación administrativa, y que incluye aspectos de firma electrónica, pero también el resto de aspectos de seguridad de la información.

2.2. Los objetivos estratégicos del Plan nacional de impulso de la seguridad de las TIC en Cataluña

El Plan se estructura alrededor de cuatro objetivos estratégicos principales:

1. Establecimiento de una estrategia nacional de seguridad TIC.

2. Apoyo a la protección de las infraestructuras críticas TIC nacionales.

3. Promoción de un tejido empresarial catalán sólido en seguridad TIC.

4. Incremento de la confianza y protección de la ciudadanía catalana en la sociedad de la información.

2.2.1. Establecimiento de una estrategia nacional de seguridad TIC

El primer objetivo trata sobre el desarrollo de una estrategia global de seguridad de la información a nivel nacional, política que se debe centrar en la necesidad de desarrollar herramientas de investigación y de concienciación del público en cuanto al número cada vez más importante de amenazas y vulnerabilidades de la seguridad en línea, definida por una aproximación multidisciplinar y con múltiples participantes, por un lado, y por una estructura de gobernanza de alto nivel, por otro.

Es preciso definir un modelo público catalán de seguridad de la sociedad de la información en Cataluña que dirija de manera global los retos que se planteen en cada momento, que actúe como interlocutor con todos los implicados y que tenga una capacidad de respuesta real a los problemas que se puedan producir, con un centro de seguridad y respuesta a incidentes como eje central vertebrador del Plan nacional de seguridad TIC, que efectúe un análisis de riesgo continuado y vele por la integridad y la continuidad de las redes y de los sistemas.

En todo caso, se debe indicar que una aproximación jerárquica, de arriba abajo, no resulta suficiente, también es necesaria la cooperación próxima de la industria y de todos los actores de la sociedad de la información, con el Gobierno como coordinador de los esfuerzos y las actividades requeridas. Al contrario, se considera que los gobiernos solos no pueden gestionar todos los retos y las cuestiones de seguridad, lo que implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes.

Este sistema reforzará iniciativas y programas ya existentes, como el Sistema público catalán de certificación, bajo responsabilidad de la Agencia Catalana de Certificación, y la actuación de otros órganos supervisores (comercio, consumo, niños y jóvenes, policías públicas, etc.).

2.2.2. Apoyo a la protección de las infraestructuras críticas TIC nacionales

El segundo objetivo estratégico se orienta a la protección de los elementos que conforman las infraestructuras críticas TIC nacional, incluyendo las redes de comunicaciones electrónicas, pero también los principales elementos en los que éstas se basan, como los sistemas de energía y los principales centros de procesamiento de datos y de prestación de servicios críticos (como la energía, el suministro de agua, el transporte, el sector financiero, las telecomunicaciones y la salud), ya que en estas infraestructuras de información confían los gobiernos, la industria, los ciudadanos y el resto de la sociedad .

Las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser múltiples. Se considera que un ataque cibernético causaría pocas víctimas o ninguna, pero podría implicar la pérdida de servicios de infraestructura vitales, como el telefónico, en el que se confía por parte de los servicios de emergencia, mientras que ataques contra los sistemas de control de infraestructuras químicas pueden implicar escapes de materiales tóxicos, que en este caso podrían producir víctimas mortales.

Por otra parte, debemos indicar que los efectos en cascada pueden ser muy dañinos y provocar grandes caídas de los servicios públicos. Algunos supuestos que hay que tratar son los servicios TIC del Gobierno de la Generalitat de Cataluña y de los gobiernos locales de Cataluña, las redes de los servicios de emergencias y de protección civil (el número único 112, los mossos, el CECOPAL, los bomberos, los agentes rurales, etc.) y los servicios privados que ofrecen apoyo.

2.2.3. Promoción de un tejido empresarial catalán sólido en seguridad TIC

El tercer objetivo estratégico persigue la creación de un tejido empresarial en seguridad TIC en Cataluña que complemente la actuación pública en esta materia y potencie el sector TIC catalán en alguno de los mercados emergentes.

Esta necesidad se ha puesto de manifiesto en el estudio sobre el mercado de las TIC en Cataluña[1], realizado por la Fundación Observatorio de la Sociedad de la Información de Cataluña (FOBSIC), que indica como línea recomendada de actuación el impulso a la pyme del sector TIC, para lo que utiliza la promoción de las certificaciones de calidad y las tecnológicas de las empresas del sector mediante programas de comunicación de las empresas clientes de los beneficios de la certificación, normativas de obligado cumplimiento en la contratación con la administración, apoyo a programas de formación y certificación en metodologías y procesos de prestación de servicios.

En este sentido, se promoverá la creación de una red de pyme para la prestación de servicios de seguridad y respuesta a incidentes de seguridad, así como una comunidad en seguridad TIC especializada en todos los aspectos de la seguridad, con una especial atención a la formación y certificación de profesionales, empresas, productos y software, en este caso basándose en las potencialidades tanto de un mercado de software libre de seguridad como de la innovación y la investigación.

Esta comunidad se debe utilizar como herramienta para la generación de negocio TIC en el territorio; por este motivo, se considera necesario ubicarlo en algún espacio adecuado para esta finalidad; en concreto, el tecnoparque de Reus.

2.2.4. Incremento de la confianza y protección de la ciudadanía catalana en la sociedad de la información

El cuarto objetivo estratégico se dirige a velar por la confianza y la protección de los ciudadanos y ciudadanas en su uso de la sociedad de la información, con una atención especial a los colectivos con más riesgos, como los niños y los jóvenes, mediante el establecimiento de programas de concienciación y apoyo específicamente dirigidos a estos colectivos.

También se actuará en apoyo de la lucha contra todas las formas de delincuencia informática, de manera coordinada con los agentes competentes y reforzando las capacidades de detección y denuncia de ilegalidades de todo tipo, así como el filtraje de contenidos y el análisis forense de evidencias electrónicas.

1. FOBSIC y Penteo Research (marzo, 2008), «El Mercat de les Tecnologies de la Informació i la Comunicació a Catalunya: 2007-2010».

Cita recomendada

ALAMILLO, Ignacio (2009). «Las políticas públicas en materia de seguridad en la sociedad de la información». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_alamilo/n9_alamillo_esp›

ISSN 1699-8154

Sobre el autor

Ignacio Alamillo

Ignacio Alamillo es consultor sénior en seguridad de la información (Dirección General de la Sociedad de la Información. Secretaría de Telecomunicaciones y Sociedad de la Información. Generalitat de Cataluña)

Licenciado en Derecho. Abogado del ilustre Colegio de Madrid. Director del Área de Asesoramiento e Investigación de la Agencia Catalana de Certificación (diciembre 2002-febrero 2008). Director del Área de Consultoría y Servicios Legales de la Agencia de Certificación Electrónica-ACE (julio 1997-diciembre 2002). Miembro del grupo directivo europeo de Seguridad de Redes y de la Información y del grupo directivo de la Iniciativa Europea de Normalización de la Firma Electrónica, con asesoramiento a la Comisión Europea. Miembro del Consejo de Certificación de ASIMELEC. Ha sido miembro del grupo directivo europeo de la Iniciativa Europea de Normalización de la Firma Electrónica y del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones. Es autor del ABC de la firma electrónica y coautor de cuatro libros sobre aspectos jurídicos de la sociedad de la información, de numerosos artículos y ponencias en firma electrónica y su campo de aplicación.

ASTREA, La Infopista Jurídica, S. L.
Blondel, 21
25002 Lleida, España

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

Facebook y los riesgos de la «descontextualización» de la información

Franck Dumortier

Fecha de presentación: julio de 2009
Fecha de aceptación: septiembre de 2009
Fecha de publicación: diciembre de 2009

Resumen

En los últimos años, ha aumentado drásticamente la participación en sitios de redes sociales virtuales (en lo sucesivo, OSNS). Servicios como los conocidísimos Facebook y Myspace, u otros como Friendster, WAYN, Bebo, Orkut de Google y muchos más cuentan con millones de usuarios registrados y no dejan de crecer. El modelo más común de estos sitios se basa en la presentación de los perfiles de los participantes y la visualización de su red de relaciones con los demás. Asimismo, las redes OSNS conectan los perfiles de los participantes con sus identidades públicas, usando nombres reales u otros símbolos de identificación del mundo real (como fotos, vídeos, direcciones de correo electrónico, etc.) a fin de permitir la interacción y comunicación entre individuos del mundo real. Por tanto, un sitio como Facebook no se puede considerar únicamente como un patio de recreo para «entes virtuales» en el que las identidades son flexibles y están desconectadas de sus «cuerpos reales». La disposición de información de registro completa, exacta y actualizada por parte de los usuarios no sólo es deseable, sino que es un requisito incluido en las condiciones de uso de Facebook. Este requisito, junto con la misión del servicio de organizar la vida social real de sus miembros, supone un incentivo importante para los usuarios, instándoles a publicar únicamente información real y válida sobre sí mismos. Una vez proporcionada esta información exacta, las interacciones en Facebook implican una amenaza para la privacidad. En este informe, argumento que el principal riesgo para la privacidad en Facebook es el de la descontextualización de la información que proporcionan los participantes. En mi opinión, esta amenaza de la descontextualización se debe a tres de las características principales de Facebook: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización en la red de Facebook. El fenómeno de descontextualización no sólo supone una amenaza para el derecho a la protección de datos, en el sentido del derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho a la privacidad como ser humano: el derecho del ser humano a ser un yo conscientemente múltiple y gregario sin una discriminación injustificada.

Palabras clave

privacidad, protección de datos, redes sociales virtuales, descontextualización de la información

Tema

Protección de datos y privacidad

Facebook and the Risks of "De-contextualization" of Information

Abstract

Participation in online social networking sites (OSNS) has increased dramatically in recent years. Services such as the well-known Facebook and Myspace but also Frienster, WAYN, Bebo, Google's Orkut and many others, have millions of registered active users and are continuously growing. The most common model for these sites is based on the presentation of the participants' profiles and the visualisation of their network of relations to others. OSNS also connect participants' profiles to their public identities, using real names and other real-world identification signs (pictures, videos, e-mail addresses, etc.) to enable interaction and communication between real-world subjects. Hence, a site like Facebook cannot be considered purely as a playground for "virtual bodies" in which identities are flexible and disconnected from "real-world bodies". Not only is the provision of accurate, current and complete registration information from the users encouraged, it is even required by Facebook's terms of use. This requirement, along with the service's mission of organizing the real social life of its members, provides major incentives for users to publish only real and valid information about themselves. This accurate information being provided, privacy threats derive from interactions on Facebook. In this paper, I argue that the main privacy risk on Facebook is the one of loss of context of the information spread by users. This de-contextualization threat is due to three major characteristics of Facebook: 1) the simplification of social relations, 2) the high level of information diffusion and 3) the network globalization and normalization effects of Facebook. This loss of context is a risk not only to data protection rights, meaning the right of the individual to control their informational identity presented in a certain context, more fundamentally it threatens the human right to privacy: the right to be a conscious, multiple and relational self not suffering any form of discrimination.

Keywords

privacy, data protection, online social networking, de-contextualization of information

Topic

Privacy and data protection

Introducción

En estos últimos años, se ha observado un aumento continuo en la participación en sitios de redes sociales virtuales (en lo sucesivo, OSNS), con una multiplicación exponencial del número de usuarios. Por ejemplo, aunque la audiencia internacional de Facebook ascendió a un total de 20 millones de usuarios en abril de 2007, el número había aumentado hasta 200 millones dos años después, con un promedio de 250.000 nuevos registros diarios desde enero de 2007. La «proporción activa» de la audiencia de Facebook también es impresionante: según las estadísticas publicadas en el sitio web, más de 100 millones de usuarios se registran en Facebook al menos una vez al día, mientras más de 20 millones de usuarios actualizan su configuración a diario, como mínimo.[1] Fundada en febrero de 2004, Facebook desarrolla tecnologías que «facilitan el intercambio de información

1. Ver estadísticas detalladas en el sitio web de Facebook: http://www.facebook.com/press/info.php?timeline

a través de un esquema social, el mapa digital de las conexiones sociales de los usuarios en el mundo real».[2] De acuerdo con la definición de danah boyd,[3] Facebook es, por tanto, un «sitio de redes sociales» en el sentido de que es un «servicio basado en la red que permite a los individuos (1) crear un perfil público o semipúblico dentro de un sistema delimitado, (2) articular una lista de otros usuarios con los que tienen conexión y (3) visualizar y entrecruzar su lista de conexiones y las realizadas por otros dentro del sistema».[4] Adicionalmente, la característica principal de un sitio como Facebook es conectar los perfiles de los participantes con sus identidades públicas, usando nombres reales y otros modos de identificación del mundo real, como fotografías, vídeos o direcciones de correo electrónico, permitiendo así la interacción y comunicación entre individuos del mundo real. Por tanto, Facebook está muy lejos de equipararse a los espacios de chat con pseudónimo y no se puede considerar únicamente como un patio de recreo para «entes virtuales» en el que las identidades son flexibles y están desconectadas de sus «cuerpos reales». De hecho, no hay casi nada virtual en lugares como Facebook. La disposición de información de registro exacta y actualizada por parte de los usuarios no sólo es deseable, sino que es un requisito incluido en las condiciones de uso. De hecho, Facebook obliga a sus usuarios a «indicar sus nombres e información reales», a mantener su «información de contacto exacta y actualizada» y les prohíbe «incluir información personal falsa».[5] Estos requisitos, junto con la misión del servicio de organizar la vida social real de sus miembros, suponen un incentivo importante para los usuarios, instándoles a publicar únicamente información real y válida sobre sí mismos. Las estadísticas son elocuentes: ya en 2005, el 89% de los perfiles de Facebook usaban nombres reales, mientras que el 61% de los perfiles incluían imágenes que permitían una identificación directa.[6]

Según las estadísticas de Facebook, cada mes se cargan más de 850 millones de fotos y 8 millones de vídeos. Además, cada semana se comparten más de 1.000 millones de unidades de contenido (enlaces en la red, noticias, entradas de blogs, notas, fotos, etc.). Dada la difusión del uso e intercambio de información personal considerada exacta y actualizada, existen importantes amenazas a la privacidad que pueden derivarse de las interacciones en Facebook, siendo la principal el riesgo de descontextualización de la información que aportan los participantes. En mi opinión, esta amenaza de la descontextualización se debe a tres de las características principales de Facebook: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización en la red de Facebook. El riesgo de descontextualización no sólo supone una amenaza para el derecho a la protección de datos, es decir, el derecho a controlar la identidad informativa que un ser humano proyecta en un cierto contexto. De un modo más fundamental, es una amenaza al derecho a la privacidad como ser humano: el derecho del ser humano a ser un yo múltiple y gregario sin una discriminación injustificada.

En la primera parte, examino las distintas características de Facebook que suponen un riesgo de descontextualización de la información en circulación. En la segunda parte, se explica por qué este fenómeno de descontextualización es una amenaza tanto para los derechos de privacidad como para la protección de datos. Finalmente, expongo que la protección de la privacidad y de los datos en Facebook no se debe centrar únicamente en las soluciones y penalizaciones para los individuos agraviados, sino en el diseño de una arquitectura que rija los flujos de datos en múltiples contextos en el sitio. Dada la importancia de la amenaza de la descontextualización, la arquitectura de Facebook debe estar diseñada de modo que evite cualquier interferencia tanto con el

2. *Ibidem*.
3. danah boyd no escribe su nombre con mayúsculas.
4. D. BOYD; N. ELLISON (2007). «Social Network Sites: Definition, History, and Scholarship». *Journal of Computer-Mediated Communication*, vol 1, n.º 13, art. 11. Disponible en línea en: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Boyd y Ellison usan «sitio de redes sociales» en lugar de «sitio de establecimiento de redes sociales» porque «los participantes no necesariamente están "estableciendo contactos" ni tratando de conocer a otras personas; en su lugar, suelen comunicarse con personas que ya forman parte de su red social más amplia».
5. Véase la «Declaración de derechos y responsabilidades» de Facebook, en: http://www.facebook.com/terms/spanish.php
6. R. GROSS; A. ACQUISTI (2005). «Information Revelation and Privacy in Online Social Networks». En: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. Pág.77.

derecho a la privacidad como con la protección de datos, siempre que dicha interferencia no sea estrictamente necesaria en un estado democrático.

1. Los riesgos de la descontextualización que se derivan de las interacciones en Facebook

En este informe, uso el término *descontextualización* para conceptualizar lo que ocurre cuando se usan comportamientos o información en un contexto distinto de aquél para el que se crearon. Tal como indica Nissembaum, el fenómeno de la descontextualización surge cuando los individuos no respetan las normas de distribución y adecuación contextuales.[7] Por ejemplo, cuando un comportamiento que sería adecuado con un amigo íntimo en un bar se muestra en público o en el trabajo, viola las normas contextuales de adecuación. Del mismo modo, si mi superior llega a conocer información dirigida originalmente a mi novia, viola las normas contextuales de distribución. Lo verdaderamente problemático en estas normas contextuales es que no admiten una definición precisa, ya que se derivan de una apreciación personal sobre el modo en que debería circular la información en el mundo físico, o, en este contexto, en el mundo real. De hecho, ambas normas de adecuación y distribución presuponen cierto entorno situacional, ya que el modo en que se divulga la información depende de propiedades muy determinadas de ese entorno, como sus características arquitectónicas, temporales e interpersonales.[8] A modo de ejemplo, no me comportaría del mismo modo con mi jefe en un bar a las 10 de la noche que en el trabajo a las 8 de la mañana, ni revelaría la misma información a las 10 de la noche en ese mismo bar con mi jefe si mi madre se uniera al grupo. Por tanto, en el mundo físico, las normas contextuales de distribución y adecuación se basan en algo típicamente humano: los sentimientos.

No obstante, como explicaré en las próximas secciones, Facebook tiene un diseño completamente distinto al del mundo físico, y sus propiedades arquitectónicas, temporales e interpersonales tienen el potencial de generar una asimetría entre los sentimientos de los usuarios y el modo en que se propaga la información. Por tanto, el uso del concepto de descontextualización es particularmente interesante en el caso de Facebook, ya que se trata de un entorno «en el que los mundos entran en colisión, donde las normas quedan atrapadas en el fuego cruzado entre comunidades, donde se derriban los muros que separan las distintas situaciones sociales».[9]

En las siguientes secciones, expondré que la amenaza de la descontextualización en Facebook se debe a tres de sus características principales: 1) la simplificación de las relaciones sociales, 2) la amplia difusión de la información y 3) los efectos de globalización y normalización de Facebook.

1.1. La simplificación de las relaciones sociales en las OSNS

Según las estadísticas publicadas en Facebook, un usuario medio tiene 120 amigos en el sitio. Ello implica que, cuando un usuario actualiza su perfil (cargando una foto o un vídeo, modificando su ideología política o creencias religiosas o cambiando su situación sentimental), publica un mensaje en su muro o responde a un test, esta información queda, por defecto y de media, a disposición de más de cien personas con las que el usuario mantiene distintos tipos de relación. De hecho, las personas con que se relaciona un usuario en Facebook pueden ser muy variadas: miembros de su familia, colegas, amantes, amigos reales, conocidos en un bar, antiguos compañeros de escuela e incluso desconocidos. Los teóricos de las redes sociales han debatido sobre la relevancia de las relaciones a distintos niveles de profundidad e intensidad en la red social de una persona.[10] Cabe destacar el hecho de

7. Véase H. NISSENBAUM (2004). «Privacy as Contextual Integrity». *Washington Law Review*, vol. 79, n.º 1.
8. C. PETERSON formuló esta misma idea en (2009). «Saving Face: The Privacy Architecture of Facebook» (borrador para comentarios – primavera de 2009). *The Selected Works of Chris Peterson*. Pág. 9. Disponible en: http://works.bepress.com/cpeterson/1
9. Véase C. PETERSON (2009). «Saving Face: The Privacy Architecture of Facebook» (borrador para comentarios – primavera de 2009). *Op.cit*, resumen.
10. Véase, por ejemplo, M. GRANOVETTER (1973). «The strength of weak ties». *American Journal of Sociology*, núm. 78, pág. 1360-1380. Véase también M. GRANOVETTER (1983). «The strength of weak ties: A network theory revisited». *Sociological Theory*, n.º 1, pág. 201-233. Strahilevitz ha destacado la relevancia de esta teoría sobre la privacidad. Véase L. J. STRAHILEVITZ (2005). «A social networks theory of privacy». *University of Chicago Law Review*, vol. 72, pág. 919.

que la aplicación de la teoría de las redes sociales a la revelación de información saca a la luz diferencias significativas entre los escenarios real y virtual (*offline* y *online*). En el mundo real, la relación entre divulgación de la información y la red social de una persona tiene, tradicionalmente, múltiples facetas: «En ciertas ocasiones, queremos que la información sobre nosotros esté sólo a disposición de un pequeño grupo de amigos íntimos, y no de desconocidos. En otros casos, estamos dispuestos a revelar información personal a extraños, pero no a quienes nos conocen bien».[11] Por ende, las redes sociales reales están formadas por lazos definibles de un modo impreciso como lazos fuertes o débiles, pero en realidad estos lazos son extremadamente diversos en lo referente al grado de cercanía e intimidad con que un sujeto percibe una relación. Las redes sociales virtuales, por otro lado, suelen reducir estas relaciones llenas de matices a relaciones binarias simplistas: «Amigo o no». En su estudio de las redes sociales virtuales, danah boyd observa que «no hay ninguna forma de determinar qué escala se ha usado o cuál es el papel o el peso de la relación. Aunque algunos usuarios están dispuestos a marcar a cualquiera como Amigo, y otras prefieren una definición conservadora, la mayoría de los usuarios tienden a incluir en esta lista a todos aquellos a los que conocen y que no les disgustan. A menudo, esto supone que se clasifica como Amigos incluso a personas a las que el usuario no conoce o en las que no confía particularmente».[12]

Cada vez más, los usuarios de Facebook tienden a clasificar como *amigos* a todas aquellas personas a las que no odian[13], y compartirán con estas relaciones una cantidad increíble de datos que podrían ser inadecuados en el contexto *heterotópico*[14] de Facebook. Tomemos, por ejemplo, a un usuario de Facebook que tiene 100 amigos: 4 de ellos son parientes, 16 son amigos íntimos, 1 amante, 4 ex amantes, 30 antiguos compañeros de colegio, 30 conocidos (de distintos contextos), 14 compañeros de trabajo y su jefe. Ahora imaginemos que nuestro usuario instala una aplicación ajena en Facebook para responder a un test divertido «¿Eres alcohólico?» y al mismo tiempo cambia su «situación sentimental» a soltero. No hay duda de que la combinación de estas informaciones tendrá un significado distinto para sus amigos y su pareja que para sus colegas, su jefe o su madre. De estas observaciones, se deriva una amenaza de descontextualización: la dificultad que tiene un ente con múltiples facetas para restringir la información que desea compartir con «Amigos» de distintos contextos. Simplificando, responder a un test «¿Cuál es tu postura sexual favorita?» puede proporcionar información interesante a mi novia pero seguramente no será adecuada para ninguno de mis compañeros de trabajo.

En este sentido, hay un punto de partida en el elemento «Listas de amigos» que proporciona Facebook y que permite a los usuarios organizar a sus amigos en distintas categorías. La herramienta les permite incluir y excluir a grupos de amigos de la posibilidad de ver partes de su perfil y contenidos. En nuestro ejemplo, un usuario cuidadoso podría agrupar a cada tipo de «amigos» en distintas categorías que haya predefinido y darles distintos niveles de acceso a informaciones tales como fotos, vídeos, situación, mensajes, etc. Sin embargo, al resolver en parte el problema de la limitación del acceso a determinadas informaciones añadiendo un control más específico, Facebook también ha introducido una mayor complejidad y trasfondo conceptual para los usuarios: ahora tienen que clasificar a sus amigos. Este es exactamente el motivo por el que no se puede considerar que las «Listas de amigos» imiten exactamente el modo en que todos limitamos el acceso de determinados amigos a cierta información personal en el mundo real. De hecho, el elemento se parece mucho más al modo en que el administrador de un sistema podría configurar las autorizaciones de uso de los recursos de un ordenador que al modo en que se desarrollan los procesos de divulgación de la informa-

11. R. GROSS; A. ACQUISTI, «Information Revelation and Privacy in Online Social Networks». Actas del *2005 ACM Workshop on Privacy in the Electronic Society*. Pág. 81.
12. D. BOYD (abril, 2004). «Friendster and publicly articulated social networking». En: *Conference on Human Factors and Computing Systems* (*CHI 2004*). Austria: Viena. Pág. 2.
13. Nótese que Hatebook.org, la versión antagónica de Facebook, se define como «*una herramienta antisocial que te desconecta de todo lo que odias*».
14. Para obtener más detalles sobre Facebook como espacio heterotópico, véase la sección 2.1, pág. 11.

ción en la vida cotidiana: el etiquetado de amigos y la creación de listas de amigos no son hechos conscientes en el mundo real.

Por tanto, la simplificación de las relaciones sociales en OSN lleva implícita una primera amenaza de descontextualización de la información teniendo en cuenta que las relaciones binarias en estos sitios pueden provocar incumplimientos de las normas contextuales de adecuación o de distribución: la divulgación de la información nunca estará tan fragmentada en el mundo virtual como lo está en el mundo real.

1.2. La amplia difusión de la información inherente a las interacciones en Facebook

No sólo la simplificación de las relaciones sociales en Facebook implica una amenaza de descontextualización, también el modo en que la información se puede difundir ampliamente a lo largo del entramado social. En el mundo real, es excepcionalmente improbable que la información sobre una persona sea interesante a más de dos grados de información. En estas situaciones, Duncan Watts observa que «cualquiera que se encuentre a mayor distancia que un amigo de un amigo es, a todos los efectos, un desconocido... Todo lo que se sitúe a más de dos grados podría estar perfectamente a mil grados de distancia».[15] En otras palabras, al menos en la era anterior a Facebook, a nadie le importaban demasiado las personas que se apartaban a más de dos grados de nosotros. Strahilevitz lo ilustra perfectamente en la siguiente cita:

«Las aventuras extramatrimoniales son actos fascinantes. Dicho eso, ninguna persona decente iría a un cóctel y le contaría una historia íntima sobre el amigo del amigo de un amigo que está teniendo una relación adúltera con alguien a quien ni hablante ni oyente conocen. Sólo si el hablante o el oyente sabe quiénes son los adúlteros o si los detalles del caso son especialmente sórdidos, divertidos o memorables, será probable que la información se difunda más allá por la red social. Y para cuando la información haya recorrido toda la cadena, parece probable que los nombres de los implicados hayan desaparecido de la historia.»[16]

Así, cuando se trate de hechos transmitidos oralmente de persona en persona, alguien debería tener una expectativa razonable de integridad contextual a más allá de dos grados en una red social. Esta norma lógica parece no sustentarse tan bien cuando uno se aleja de las comunicaciones del mundo real e interactúa en servicios de redes virtuales como Facebook, por cinco razones principales.

La primera es que la difusión de la información a lo largo del esquema social se ve impulsada por la presencia de una red visible de amigos en el perfil de cada participante. Mientras que en el mundo real los amigos pueden pasar años sin saber que comparten un amigo mutuo, en Facebook pueden averiguar con gran facilidad quiénes son sus amigos comunes. Esta lista también hace que sea más fácil para todos saber quiénes son los amigos del amigo de un amigo propio. Además, cada perfil de la lista de amigos de un amigo se puede «compartir» y comentar en el perfil del usuario. A modo de ejemplo, yo puedo ojear mi lista de relaciones, elegir a uno de mis amigos, ver quiénes son sus amigos, después pasar a los amigos de sus amigos y finalmente publicar el perfil limitado de uno de ellos en mi perfil con un comentario desafortunado que se puede seguir compartiendo y comentando a lo largo de los esquemas sociales de mis propios «amigos».

En segundo lugar, Facebook está formado por miles de redes en todo el mundo, y se anima a los usuarios a unirse a ellas para conocerse y hacer amigos entre las personas de su área. Las mayores de estas redes son las conocidas como «redes geográficas», de las que la belga aúna a más de 780.000 personas. Una vez se une a una de estas redes, un usuario puede clasificar a los usuarios de la misma red usando criterios como el sexo, la edad, la situación sentimental, sus intereses o su ideología política. Además, dependiendo de la configuración de privacidad de la persona objetivo, los usua-

15. D. J. WATTS. *Six Degrees: The Science of a Connected Age*. Nueva York: Norton. Pág. 299-300.
16. L. J. STRAHILEVITZ. *Op.cit*. Pág. 47.

rios pueden acceder a la totalidad o a parte de los perfiles de los amigos de los amigos de sus amigos.[17]

Otro factor que podría causar una amplia difusión de la información es la opción de etiquetado que propone Facebook. Una etiqueta es una palabra clave, a menudo el nombre real de un participante asociado o asignado a una unidad de información (una foto, un vídeo, etc.) para describir al individuo y permitir una clasificación y la búsqueda de información sobre la base de la palabra clave. Cuando se asocia a una foto o a un vídeo, la etiqueta proporciona un acceso directo al perfil del usuario representado. Aquí aparece el clásico problema de Facebook: bajas la guardia durante unas horas en una noche (o un día) y alguien cuelga las fotos (o vídeos) del momento para que las vean todos los amigos de un amigo, no sólo tus amigos íntimos que compartieron ese momento contigo. De hecho, Facebook no ha creado un ajuste de privacidad por defecto que permita a los usuarios aprobar o rechazar etiquetas de fotos antes de que puedan aparecer en el sitio.[18]

Una cuarta preocupación por la difusión involuntaria de información se deriva de la Plataforma Facebook desde el móvil. Según las estadísticas de Facebook, *«actualmente hay más de 30 millones de usuarios activos que acceden a Facebook a través de sus dispositivos móviles.. Los usuarios que usan Facebook en sus dispositivos móviles son casi un 50% más activos en Facebook que los usuarios de otros tipos de equipos»*.[19] La mayor amenaza para la privacidad que implica esta herramienta se deriva de la ubicuidad de los dispositivos móviles, que tienen el potencial de permitir que la información virtual acceda al mundo real en cualquier momento, en cualquier lugar y en cualquier ocasión. De hecho, en el mundo real no importan los ajustes de privacidad: con su móvil, uno de mis amigos del mundo real podría mostrarme fácilmente el perfil completo en Facebook de uno de sus «amigos», al que no conozco en absoluto, sólo porque una de sus características es interesante en el contexto de nuestra conversación personal.

Por último, la introducción de aplicaciones de terceros en Facebook ha expuesto los datos personales de los usuarios ante un grupo creciente de diseñadores y comercializadores. Según un estudio realizado en 2007,[20] de las 150 aplicaciones principales de Facebook, cerca del 91% tenía acceso a datos personales innecesarios. Dada la naturaleza recreativa de muchas aplicaciones principales, probablemente esta estadística no ha cambiado drásticamente. Los usuarios se han acostumbrado a autorizar incluso aplicaciones simples y no saben qué datos se van a usar y a quién se van a transferir antes de autorizar una aplicación. «We're Related» *(somos familia)* es una de estas aplicaciones ajenas fuente de estas preocupaciones. Según un informe, esta aplicación, que dice tener 15 millones de usuarios activos cada mes, trata de identificar y enlazar a miembros de una familia que ya estén en la red, aunque su parentesco sea muy lejano: «Se solicita a los nuevos usuarios que den carta blanca a la aplicación para que "acceda a su información del perfil, fotos, la información de sus amigos y todos los contenidos que requiera para funcionar". La aplicación parece autorizarse a sí misma para proporcionar esta información a cualquier otro participante de Facebook –aunque los usuarios hayan establecido unos parámetros de privacidad más

17. En 2007, la empresa de seguridad y control de TI, Sophos, reveló que los miembros exponían imprudentemente sus datos personales de forma masiva a millones de extraños, exponiéndose ellos mismos a un riesgo de robo de identidad. La empresa de seguridad realizó una elección aleatoria de 200 usuarios en la red de Facebook en Londres, que es la mayor red geográfica del sitio, con más de 1,2 millones de miembros, y detectó que un impresionante 75 por ciento permitió que cualquiera visionara su perfil, independientemente de si lo habían puesto o no a disposición de sus amigos. Sophos vió evidencias de que los usuarios de Facebook en otras regiones geográficas exhiben de un modo similar su información personal ante perfectos desconocidos. La razón de esta divulgación involuntaria de la información era que, aun cuando se hubiera configurado previamente el grado de privacidad para asegurarse de que sólo los amigos accedieran a la información, al unirse a una red, el perfil se abría automáticamente a cualquier otro miembro de la red. Hasta 2009, Facebook no cambió su configuración de identidad por defecto para las redes geográficas a fin de evitar la exposición involuntaria de los perfiles.
18. Existe la posibilidad de restringir indirectamente la visibilidad de las fotos etiquetadas visitando primero la página de privacidad de tu perfil y modificando el parámetro junto a «Fotos en las que se te ha etiquetado», eligiendo la opción «Personalizar» y después la opción «Sólo yo» y «Ninguna de mis redes». Si deseas que las fotos etiquetadas sean visibles para ciertos usuarios, puedes incluirlos en el cuadro bajo la opción «Algunos amigos». En el cuadro que aparece después de elegir «Algunos amigos», puedes introducir a amigos individuales o listas de amigos.
19. Véanse las estadísticas de Facebook en: http://www.facebook.com/press/info.php?statistics
20. A A. FELT; D. EVANS (mayo, 2008). «Privacy Protection for Social Networkin APIs». *W2SP*. Disponible en http://www.cs.virginia.edu/felt/privacybyproxy.pdf

estrictos a fin de limitar el acceso a sus datos personales.»[21] Sin embargo, tal como se indica en los términos de uso de Facebook, la empresa no asume ninguna responsabilidad por las prácticas inadecuadas acerca de la privacidad de los diseñadores de aplicaciones externas.[22]

Combinados, estos cinco factores implican un riesgo de difusión involuntaria de los datos más allá de las expectativas razonables de integridad contextual de los usuarios de Facebook, ya que la información importante compartida con sus «amigos» puede propagarse más allá de dos niveles de conexión.

En la siguiente sección, expondré que esta amenaza de descontextualización puede verse incrementada por los efectos de globalización y normalización de Facebook.

1.3. Los efectos de globalización y normalización de Facebook

Todos hemos experimentado el incremento en la presión de nuestras relaciones para que nos hagamos por fin con el programa y nos unamos a la red. En parte, se puede explicar por el hecho de que cuando alguien se registra en Facebook, el sitio invita al nuevo usuario a «averiguar cuáles de sus contactos por email están ya en Facebook». Entonces Facebook pide a los usuarios que introduzcan su dirección de email y contraseña para muchos de los principales proveedores de servicios de correo electrónico (Yahoo, Hotmail, Gmail, etc.). A continuación, Facebook se registra en la cuenta y se descarga todos los contactos. Los usuarios ven una lista de los individuos que actualmente son miembros de Facebook, y tienen la posibilidad de enviar solicitudes de amistad a cada uno de ellos. Aparece una pantalla con todos los contactos preseleccionados. Ahora, el usuario tiene la opción de invitar a todos sus otros contactos a unirse a Facebook.[23] Por defecto, se preseleccionan todos los contactos: por tanto, el comportamiento por defecto es enviar mensajes a todos los contactos invitándoles a ser amigos en Facebook.

Los incentivos para unirse al programa se concretan aún más cuando se examina la función de «etiquetado» propuesta por Facebook. Un elemento problemático de esa función es que se puede etiquetar a personas que no se hayan registrado en la red (por tanto, a los denominados amigos, a perfectos desconocidos e incluso a enemigos). Por supuesto, se puede ejercer el derecho de acceso y el derecho de rectificación/borrado si alguien desea eliminar una etiqueta en particular de uno mismo, pero primero debe registrarse en Facebook. Esto es lo que podríamos denominar el efecto de globalización de Facebook: sin estar en el programa, uno puede ser un objeto de datos definido por fotos y artículos. Incluso sin conocerlo y sin ser capaz de reaccionar, uno puede ser un tema de conversación ampliamente difundido y bien documentado. Para convertirse en un individuo de datos reales, el objeto de los datos debe registrarse en Facebook antes de poder ejercer sus derechos de protección de datos. Para poder ser actores activos en el control de su identidad informativa, los usuarios están obligados a registrarse en el programa.

Dado el impresionante crecimiento de Facebook (314% el año pasado), el servicio se está convirtiendo, cada vez más, en una herramienta de comunicación diaria, en la que, por ejemplo, está registrado el 21% de la población belga.[24] Paradójicamente, cada vez es más raro no estar en Facebook que lo contrario. Esto es lo que podríamos denominar el efecto de normalización de Facebook: un futuro en que los empresarios se pregunten lo siguiente: «¿por qué el Sr. X no está en Facebook? Es raro... ¿tiene algo que ocultar?», quizá no sea tan lejano.

21. Véase R. WATERS (2009). «Facebook applications raise privacy fears». *Financial times online*. Disponible en http://www.ft.com/cms/s/0/2a58acfa-5c35-11de-aea3-00144feabdc0.html
22. Véanse los Términos de Uso de las Aplicaciones de la Plataforma Facebook: «Cuando instala una Aplicación de Desarrollador, o Developer Application, entiende que dicha Aplicación no ha sido aprobada, asignada ni revisada en modo alguno por Facebook, y que no somos responsables de su uso o incapacidad de uso de tales aplicaciones, incluyendo, sin limitación, el contenido, la exactitud o fiabilidad de dicha Aplicación de Desarrollador ni las prácticas de privacidad u otras políticas del Desarrollador. USE ESTAS APLICACIONES DE DESARROLLADOR POR SU CUENTA Y RIESGO». Disponible en: http://developers.facebook.com/user_terms.php
23. Véase http://epic.org/privacy/facebook/
24. Véanse las estadísticas en http://katrin-mathis.de/wp-mu/thesis/

Una vez descritas las tres características principales de Facebook que implican un riesgo de descontextualización de la información personal, en la siguiente sección, analizaré las consecuencias de tal amenaza respecto a los derechos de privacidad y protección de datos.

2. Consecuencias de la amenaza de descontextualización sobre los derechos a la privacidad y a la protección de datos

Las tres características de Facebook que he presentado –simplificación de las relaciones sociales, amplia difusión de la información y efectos de globalización y normalización– pueden implicar riesgos importantes de descontextualización de la información. Tal amenaza de descontextualización de la información personal en Facebook puede afectar tanto al derecho a la privacidad como al derecho a la protección de datos de los usuarios del servicio.

Las conexiones entre ambos derechos ya han sido objeto de rigurosos análisis por parte de autores de renombre.[25] A los efectos de nuestro debate, tomemos como punto de partida el mero hecho de que el derecho a la privacidad se ha considerado tradicionalmente un derecho humano reconocido a los seres humanos, mientras el derecho a la protección de datos se concede a los sujetos de datos a través de los instrumentos legales más significativos a escala europea. De hecho, aunque la privacidad y el Tribunal Europeo de los Derechos Humanos giran en torno al ser humano, la directiva 95/46 habla de sujetos de datos. ¿Por qué? La cuestión podría parecer simplista o trivial, pero entender desde este punto de vista los significados respectivos del derecho a la privacidad y a la protección de datos nos podría ayudar, en mi opinión, a entender el modo en que la descontextualización de la información supone una amenaza para ambos derechos.

2.1. Consecuencias de la amenaza de la descontextualización sobre la Privacidad como un derecho del ser humano

Cabe recordar que la privacidad es un derecho otorgado a los seres humanos y puede parecer trivial, sin embargo, el término *humano* es extremadamente ambiguo y ha experimentado una extraordinaria evolución histórica y filosófica. A fin de presentar adecuadamente este tema y evitar debates innecesarios, limitémonos a reconocer que un ser humano no se puede reducir a un cuerpo o a una persona física. Naturalmente, en un estado ideal, deberían concederse derechos humanos a todos los cuerpos con especificaciones humanas definidas por la anatomía, pero, históricamente, no cabe duda de que los legisladores también estaban influidos por las concepciones filosóficas del *ser interior* cuando diseñaron el marco de los derechos humanos. A modo de ejemplo, el artículo 1 de la Declaración Universal de los Derechos Humanos define al ser humano como «dotado de razón y consciencia», recuperando un punto de vista muy kantiano según el cual la característica definitiva del ser humano era su capacidad de raciocinio. La razón, según Kant, permitía al ser entender y ordenar el mundo con certeza. En consecuencia, el yo kantiano se concebía como un pilar de identidad de subjetividad coherente, que sobresale en la corriente de la experiencia cambiante. No obstante, la noción modernista liberal del yo como un individuo unitario, estable y transparente ha sido objeto de una crítica cada vez más intensa a lo largo del siglo veinte. De hecho, muchas teorías del modernismo tardío o postmodernistas sobre el yo afirman que es múltiple y fraccionado. En consecuencia, el yo es una noción ilusoria interpretada como algo estático y unitario, pero completamente fluida en la realidad.[26] La evolución de estas reflexiones ha llevado a conceptos del ser humano como un «yo múltiple»[27] *relacional, subjetivo y dependiente del contexto*. La idea de Goffman, llena de matices, de una persona cosmopolita refleja perfectamente el debate filosófico entre unificación y fragmentación del yo moderno que evoluciona constantemente en una pluralidad de contextos. Según él,

25. Gutwirth y De Hert, por ejemplo, han debatido la distinción considerando el derecho a la privacidad como una especie de «*herramienta de opacidad*» mientras, según los autores, el derecho a la protección de datos sería una «*herramienta de transparencia*». Véase S. GUTWIRTH; P. DE HERT (2006). «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power». En: E. CLAES; A. DUFF; S. GUTWIRTH (eds.) (2006). *Privacy and the criminal law*. Amberes: Intersentia. Págs. 61-104.

«En muchas situaciones modernas, los individuos se ven atrapados en una variedad de contextos dispares... cada uno de los cuales puede requerir diferentes formas de comportamiento «adecuado»... Cuando el individuo sale de un contexto y entra en otro, ajusta la «presentación del yo» con relación a lo que se requiere en una situación particular. A menudo, se piensa que este punto de vista implica que un individuo tiene muchos yos, al igual que existen contextos de interacción divergentes... Sin embargo, no sería correcto ver la diversidad contextual como algo que simple e inevitablemente promueve la fragmentación del yo, y mucho menos su desintegración en múltiples «yos». En muchas circunstancias, incluso puede promover una integración del yo... Una persona puede usar la diversidad para crear una identidad propia distintiva que incorpore de forma positiva elementos de distintas situaciones en un discurso integrado. Por tanto, una persona cosmopolita es precisamente la que logra sentirse a gusto en una variedad de contextos.»[28]

Más allá del dilema postmoderno entre unificación y fragmentación del yo, lo importante a los efectos de nuestro debate es el hecho de que los seres humanos son concebidos, cada vez más, como seres contextuales en constante reinvención de sí mismos, que adoptan distintos papeles, posturas y actitudes en una compleja red de redes abierta a los demás. Teniendo en cuenta esta evolución conceptual del yo humano hacia un yo contextual, es interesante analizar la evolución del significado de su derecho a la privacidad.

Desde su aceptación como «derecho a ser dejado en paz»,[29] el derecho a la privacidad ha experimentado evoluciones significativas. Es interesante que el Tribunal Europeo de Derechos Humanos haya afirmado que sería demasiado restrictivo limitar la noción de vida privada a un círculo interior en el que el individuo puede vivir su propia vida personal del modo que elija y excluirse en él de todo el mundo exterior no incluido en ese círculo: *«El respeto por la vida privada también debe incluir hasta cierto punto el derecho a establecer y desarrollar relaciones con otros seres humanos»*.[30] Naturalmente, ahora la privacidad se concibe como un fenómeno que tiene en cuenta las relaciones entre un yo y su entorno/otros yos. Como observa Fried:

«La privacidad no es sólo un medio posible entre muchos de asegurar otro valor, sino que está necesariamente relacionada con los fines y las relaciones del tipo más fundamental: respeto, amor, amistad y confianza. La privacidad no sólo es una buena técnica de continuación de estas relaciones fundamentales, que son más bien inconcebibles sin privacidad. Requieren un contexto de privacidad o la posibilidad de gozar de privacidad para existir.»[31]

Además, dado que los «usuarios tienen, y es importante que mantengan, diferentes relaciones con usuarios diferentes»,[32] las relaciones entre los yos son, por naturaleza, extremadamente contextuales. Por tanto, Nissenbaum afirmó que el valor definitivo que debe proteger el derecho a la privacidad es la integridad contextual[33] de un yo contextual dado con diferentes comportamientos y que comparte información diferente en función del contexto en el que evoluciona. A este respecto, Rachels observa que:

«Hay una cercana relación entre nuestra capacidad de controlar quién tiene acceso a nosotros y a la información sobre nosotros y nuestra capacidad de crear y mantener

26. Véase, por ejemplo, K. P. EWING (1990). «The Illusion of Wholeness: Culture, Self, and the Experience of Inconsistency». *Ethos*, vol. 18, n.º 3, págs. 251-278 (donde se argumenta que los usuarios «proyectan múltiples representaciones incoherentes de sí mismos que dependen del contexto y pueden variar rápidamente»); A. P. HARRIS (1996). «Foreword: The Unbearable Lightness of Identity». *Berkeley women's law journal*, vol. 11, págs. 207-211 (donde argumenta que el problema con cualquier teoría general de la identidad «es que la "propia identidad" tiene poca sustancia»); J. WICKE (1991). «Postmodern Identity and the Legal Subject». *University of Colorado Law Review*, vol. 62, págs. 455-463 (donde se observa que un concepto postmodernista de la identidad reconoce el yo como fragmentado y captura «sus grietas causadas por la miríada de discursos sociales que lo conforman»).
27. Véase, p. ej. J. ELSTER (1986). «The Multiple Self». *Studies in Rationality and Social Change*. Cambridge University Press.
28. GOFFMAN, citado en A. GIDDENS (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press. Pág. 189.
29. WARREN y BRANDEIS (1890). «The right to privacy». *Harvard Law Review*, vol. 4, n.º 5.
30. Véase, p. ej. ECHR (dic, 1992). *Niemietz v. Germany*. N.º A 251-B, § 29.
31. C. FRIED (1968). «Privacy». *Yale Law Journal*, n.º 77, págs. 475-493.
32. F. SCHOEMAN (1984). «Privacy and Intimate Information». *Philosophical Dimensions of Privacy: an anthology*. Pág. 403-408.
33. H. NISSENBAUM. *Op.cit*..

diferentes tipos de relaciones sociales con usuarios diferentes... es necesario tener privacidad si vamos a mantener la variedad de relaciones sociales con otros usuarios que queremos tener y por eso es importante.»[34]

Análogamente, Agre definió el derecho a la privacidad como «la ausencia de límites no razonables en la construcción de la identidad propia».[35] Dado que la construcción de la identidad de uno se concibe cada vez más como una integración autonómica y narrativa progresiva de distintos elementos derivados de una diversidad contextual, muchos autores tienden a considerar el derecho a la privacidad como un derecho a la autodeterminación, una condición importante para la autonomía individual.[36] En otras palabras, al igual que las relaciones con los demás son esenciales para construir la personalidad de un individuo, el derecho a la privacidad también impulsa el propio desarrollo[37] al proteger una serie de relaciones contextualizadas de intrusiones o fugas no razonables. En esta perspectiva, el derecho a la privacidad se puede concebir como «un derecho a la autodeterminación del yo contextual» que le garantiza la posibilidad de actuar y comunicarse como desee contextualmente sin tener que temer una descontextualización inadecuada de sus comportamientos o de la información.

Imaginemos un padre de 45 años que trabaja como empleado en un banco, participa políticamente en un partido antimilitarista de izquierdas, va a cazar los sábados con sus amigos, va a la iglesia todos los domingos con su familia y le gusta mirar el Playboy los lunes con unos amigos durante el descanso matinal. Cabría pensar que algunas de estas representaciones del yo dependientes de un contexto son incoherentes o incompatibles entre sí. También es fácil imaginar cuán inadecuado puede parecer un comportamiento o una información de uno de estos contextos en otro de los contextos dados. Pero, lo que es fundamental, todos estaremos de acuerdo en que ninguno de estos contextos o situaciones son ilegales o nocivos *per se*. Este es exactamente el objeto del derecho a la privacidad: mostrar *respeto* por la autonomía individual, aunque la construcción de la identidad intercontextual de alguien nos pueda parecer incoherente. Desde este punto de vista, el derecho a la privacidad no sólo es una condición importante de la autonomía individual sino, en un sentido más general, de la supervivencia de una democracia auténtica. Antoinette Rouvroy proporciona una de las versiones mejor informadas de esta idea:

«El derecho a la privacidad garantiza la posibilidad de un sujeto de pensar de forma diferente a la mayoría y de revisar sus preferencias de primer orden. Por tanto, la privacidad es una condición de la existencia de «sujetos» capaces de participar en una democracia conversadora. En consecuencia, la privacidad también protege estilos de vida legales pero poco populares contra las presiones sociales para que se adapten a las normas sociales dominantes. La privacidad, en tanto que ausencia de límites no razonables en la construcción de la propia identidad, sirve para evitar o combatir la «tiranía de la mayoría». El derecho a la privacidad y el derecho a no ser discriminado tienen en común que protegen las oportunidades de que los individuos experimenten una diversidad de formas de vida no convencionales. La privacidad en sí es una herramienta para evitar discriminaciones y prejuicios».[38]

El derecho a la privacidad, por tanto, se puede conceptualizar como un derecho a la integridad contextual que protege la posibilidad que tiene cualquiera de construir su propia identidad a través de relaciones diferenciadas. El objetivo de este derecho a la diferencia es garantizar la multiplicidad, la creación, la novedad y la invención en una sociedad democrática y evitar el inmovilismo o una fuerte normalización estéril. Por eso, la descontextualización de la información personal se puede considerar como una de las amenazas principales para el derecho a la privacidad.

34. J. JAMES (1975). «Why Privacy Is Important». *Philosophy and Public Affairs*, vol. 4, n.º 4, págs. 323-333.
35. P. E. AGRE; M. ROTENBERG (eds.) (1998). «Technology and Privacy. The New Landscape». *MIT Press*. Pág. 3.
36. Véase, p. ej. A. ROUVROY; Y. POULLET (2009). «The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy». En: S. GUTWIRTH; P. DE HERT; Y. POULLET (eds.). *Reinventing Data Protection*. Springer.
37. Véase ECHR (febr., 2003). *Odièvre v. France*, donde el tribunal reconoció que el derecho a la privacidad (artículo 8 de la Convención Europea sobre Derechos Humanos) protege, entre otros intereses, el derecho al desarrollo personal.
38. A. ROUVROY (2008). «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence». *Studies in Ethics, Law, and Technology*, vol. 2, n.º 1, pág. 34.

Esta amenaza de descontextualización está particularmente presente en el caso de Facebook, dado que es una plataforma de contextos colapsados. De hecho, el servicio funde cualquier relación posible en un único espacio social: amistad, política, trabajo, amor, *etc.*, todas se mezclan en un entorno único. Por tanto, se puede considerar que Facebook es lo que Foucault denomina heterotopía. Según el filósofo,

«Las heterotopías son anti-sitios, una especie de utopía hecha realidad en la que los sitios reales, todos los demás sitios reales que se pueden encontrar en una cultura, se representan, objetan e invierten simultáneamente. Los lugares como éste están fuera de cualquier lugar, aunque sea posible indicar su ubicación en la realidad».[39]

Esta definición, aplicada a Facebook, revela toda su precisión. De hecho, los servidores de Facebook están situados en algún lugar de EE.UU., por lo que se puede indicar su ubicación en la realidad.Además, al igual que las heterotopías, Facebook «*puede yuxtaponer en un único lugar real varios lugares incompatibles entre sí*».[40] En este sentido, se puede considerar que Facebook está fuera de todos los lugares. De hecho, mientras en el mundo físico las puertas regulan la entrada, los muros amortiguan el sonido, las cortinas bloquean las miradas curiosas, mientras podemos modular el volumen de nuestra voz durante una conversación dependiendo de cuán delicado sea el contenido y quién pueda oírlo, la arquitectura descontextualizadora de Facebook está por encima del espacio y, por tanto, dificulta en gran medida ajustar nuestra presentación para adecuarla a diferentes situaciones.[41] Por tanto, la arquitectura heterotópica de Facebook tiene el potencial de generar una asimetría entre la audiencia que imagina un usuario y su audiencia real, simplemente porque la plataforma carece de separación de espacios. Con ello, el servicio dificulta aún más a los usuarios la evaluación de qué normas contextuales de adecuación o distribución deberían esperar que se respeten cuando se divulga información en el sitio.

Es aquí donde el fenómeno de la descontextualización en Facebook amenaza el derecho a la privacidad: amenaza la posibilidad del ser humano de actuar como un yo contextual y relacional y le impide construir su propia identidad a través de relaciones diferenciadas. Con ello, Facebook también puede causar discriminaciones y prejuicios importantes.

2.2. Consecuencias de la amenaza de la descontextualización sobre la protección de datos como un derecho de los sujetos de datos

El fenómeno de la descontextualización en Facebook no sólo amenaza al derecho a la privacidad de los seres humanos, sino también al derecho a la protección de datos de los sujetos de datos. De hecho, aunque el derecho a la privacidad trata sobre seres humanos, los instrumentos más importantes de protección de datos crean derechos para sujetos de datos. La directiva 95/46 define un sujeto de datos como una persona natural identificada o identificable y a una persona identificable como una que se puede identificar, directa o indirectamente, sobre todo con referencia a un número de identificación o a uno o varios factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. Así, un «sujeto de datos» se concibe como alguien que se puede identificar sobre la base de uno o varios factores específicos de *un aspecto* de su identidad. Por eso, Agre define el derecho a la protección de datos como «el derecho a controlar un aspecto de la identidad que uno proyecta hacia el mundo».[42] Es interesante que el derecho a la protección de datos se pueda considerar una forma de control sobre una proyección *parcial* de la «identidad» de uno, que, como ya se ha mencionado, es extremadamente *contextual* y *relacional*.

Por este motivo, creo que el derecho a la protección de datos se puede conceptualizar como un derecho otorgado a «dividuos». Registrado desde que se publicara el primer diccionario de Noah Webster (1828) hasta la actualidad, el término *dividuo* significa *dividido, compartido o participado, en común con otros*. El Random House Unabridged Dictionary ofrece los siguientes significados: 1) divisible o

39. M. FOUCAULT (1967). «Of Other Spaces». *Heterotopias*.
40. *Ibidem*.
41. Se puede encontrar la misma idea en C. PETERSON (2009). «Saving Face: The Privacy Architecture of Facebook» » (borrador para comentarios – primavera de 2009). *Op. cit.* Pág. 9 y 35.
42. P. E. AGRE; M. ROTENBERG (eds.) (1998). «Technology and Privacy. The New Landscape». *MIT Press*. Pág. 3.

dividido; 2) separado, distinto; 3) distribuido, compartido. Por ende, la palabra *dividuo* implica tanto el significado de compartido como el de dividido, características básicas de las *relaciones contextuales* en las que el contenido diferenciado se comparte en función de con quién se está comunicando. Asimismo, Deleuze usa el término *dividuo* en su descripción de las sociedades del control «que ya no operan confinando a los usuarios sino a través del control continuo y la comunicación instantánea».[43] Para Deleuze, la sociedad contemporánea ha causado una crisis generalizada en la que los espacios de enclaustramiento convierten a los usuarios en «*dividuos*» de datos. Según el filósofo,

«Las sociedades disciplinarias tienen dos polos: la firma que identifica al individuo y el número o la numeración administrativa que indica su posición dentro de una masa. En las sociedades de control, por otro lado, lo importante ya no es la firma o el número, sino un código: el código es una contraseña de acceso, mientras las sociedades disciplinarias están reguladas por términos de vigilancia (tanto desde el punto de vista de la integración como del de la resistencia). El lenguaje numérico del control está formado por códigos que marcan el acceso a la información o lo deniegan. Ya no nos encontramos tratando con el binomio masa/individuo. Los individuos se han convertido en «dividuos» y las masas en muestras, datos, mercados o bancos.»[44]

Tal como ilustra la cita, una de las características de las sociedades de control es la emergencia de «dividuos» concebidos como «seres humanos corpóreos infinitamente divisibles y reductibles a representaciones de datos mediante las modernas tecnologías de control, como sistemas basados en el ordenador».[45] Tal como escribe Williams, a través de los datos que se obtienen sobre nosotros, las tecnologías de control pueden separar quiénes somos y lo que somos de nuestros yos físicos. Los datos se convierten en representaciones de nosotros dentro de la red de relaciones sociales; los datos son los indicadores de nuestros hábitos y preferencias. Adoptando el término de Laudon, podemos hablar de nuestras «imágenes en datos»:[46] dado que no estamos presentes físicamente, existe el riesgo de que se nos reduzca a nuestros intereses y comportamientos documentados. Tal como indica Williams, «esto implica el riesgo de que los complejos procesos de autodeterminación se concreten en unas pocas fórmulas en un soporte de almacenamiento electrónico. La separación de nuestros yos y nuestras representaciones trae a la luz un segundo aspecto de nuestra dividualidad. Como datos, somos clasificables de diversas maneras: se nos incluye en diferentes categorías, y se nos evalúa con distintos fines. Por tanto, nuestra divisibilidad pasa a ser la base de nuestra clasificabilidad en categorías delimitadas, útiles e incluso beneficiosas para terceros que manipulan los datos».[47] En tercer lugar y de forma fundamental, dada la divisibilidad de nuestras imágenes de datos en varios contextos de representación, los «dividuos contextuales» están cada vez más amenazados por el riesgo de la descontextualización. De hecho, dada la extrema fluidez de los datos electrónicos, la información obtenida en un contexto situacional puede ser reutilizada en otro sentido, a veces muy inapropiado.

Teniendo en cuenta estas amenazas diversas que resultan de nuestra creciente divisibilidad, creo que la regulación europea para la protección de datos se diseñó para dotar a los «dividuos» de los medios necesarios para controlar la imagen informativa que proyectan en su «contexto dividual» estableciendo principios generales de protección de datos y proporcionando derechos a los «sujetos de datos». En otras palabras, los «sujetos de datos» se pueden considerar «dividuos» con medios legales para desafiar a cualquier descontextualización de la información procesada sobre ellos. Se pueden encontrar ejemplos concretos de sus medios con relación a su ima-

43. G. DELEUZE (oct., 1992). «Postscript on the Societies of Control». *MIT Press*. Cambridge, MA. Págs. 3-7. Disponible en: http://www.spunk.org/texts/misc/sp000962.txt
44. *Ibidem*.
45. R. W. WILLIAMS (2005). «Politics and Self in the Age of Digital Re(pro)ducibility». *Fast Capitalism*, vol. 1, n.º 1. Disponible en: http://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html
46. Véase L. KENNETH (1986). *The Dossier Society: Value Choices in the Design of National Information Systems*. Nueva York: Columbia U.P.
47. R. W. WILLIAMS. *Op.cit*.

gen informativa contextual en la Directiva 95/46. En primer lugar, y lo más importante, el artículo 6 obliga al procesamiento de datos «con fines especificados, explícitos y legítimos y no se podrán procesar más allá de ningún modo incompatible con estos fines». En cierto sentido, el principio de limitación de fines conecta una protección adecuada para los datos personales con las normas de información de los contextos específicos, exigiendo a los controladores de datos que estos datos no se distribuyan más allá cuando este nuevo flujo no respete las normas contextuales. El mismo artículo de la Directiva también requiere que los datos sean «adecuados, relevantes y no excesivos con relación al fin para el que se obtienen y/o procesan», exigiendo que la obtención y difusión de la información sean *adecuadas* para ese contexto y obedezcan las normas de información aplicables en él. Estos dos principios de la Directiva Europea (limitación de los fines y calidad de los datos) se pueden interpretar como la consagración de la teoría de Helen Nissembaum, según la cual «una normativa sobre la privacidad en términos de integridad contextual afirma que se ha producido una violación de la privacidad cuando se incumplen las normas contextuales de adecuación o de distribución».[48] En consecuencia, los derechos de información, acceso, rectificación y oposición se pueden considerar medios legales de atribución a «dividuos contextuales» para que se enfrenten a cualquier incumplimiento de las normas contextuales (de adecuación o distribución) por parte de los controladores de datos.

En resumen, mientras que el derecho a la privacidad garantiza al ser humano la posibilidad de contar con muchas facetas y actuar de forma contextualmente diferente a fin de asegurar la perseverancia de una democracia vívida y que permita el debate, el derecho a la protección de datos se puede considerar una herramienta para dotar a los «dividuos contextuales» de medios para asegurar la integridad contextual de su imagen informativa.

A mi parecer, conceptualizar el derecho a la protección de datos como derecho de «dividuos contextuales» puede ayudarnos a entender por qué el fenómeno de la descontextualización es tan especialmente dañino para nuestros derechos de protección de datos en un sitio como Facebook. De hecho, uno de los principales efectos de los entornos heterotópicos como Facebook es la recomposición artificial de los individuos. Citando a Foucault,

«No se debe concebir al individuo como una especie de núcleo elemental, un átomo primitivo, un material múltiple e inerte sobre el que se aplica energía o con la que parece colisionar y, al hacerlo, se fragmenta o subdivide a los individuos. De hecho, uno de los efectos primordiales de la energía es que ciertos cuerpos, ciertos gestos, ciertos discursos, ciertos deseos se identifican y constituyen como individuos. El individuo, por tanto, no es el vis-a-vis de la energía, es, en mi opinión, uno de sus efectos primordiales».[49]

En Facebook, la información personal que publica un usuario, combinada con los datos que perfilan las acciones e interacciones de los usuarios con otras personas, puede crear un perfil muy rico de los intereses y actividades de esa persona. La recogida multi-contextual de todas mis contribuciones y las de mis amigos puede generar fácilmente una imagen individual de mí. Por tanto, al fusionar todos los contextos posibles en un único entorno de información, Facebook niega la existencia de nuestras dividualidades y, en consecuencia, niega nuestros derechos como dividuos.

En otras palabras, la finalidad descrita en la página principal de Facebook –«Facebook te ayuda a comunicarte y compartir tu vida con las personas que conoces»– es excesivamente amplia como para determinar qué datos son adecuados, relevantes y no excesivos con relación a dicha finalidad. Si la arquitectura de Facebook elimina la integridad contextual, es porque las características más fundamentales de su diseño entran directamente en conflicto con las normas de distribución y adecuación. De hecho, la multi-contextualidad global no se puede cubrir con un derecho a la protección de datos porque, cuando la finalidad de un servicio se define como «todo», todos los datos se pueden considerar adecuados, relevantes y no excesivos y cualquier distribución ulterior se puede considerar compatible.

48. H. NISSENBAUM (2004). «Privacy as Contextual Integrity». *Washington Law Review*, vol. 79, n.º 1, pág.138.
49. M. FOUCAULT. «Body/Power». En: Colin GORDON (ed.). *Foucault on Power/Knowledge: Selected Interviews and other writings 1972-1977*. Londres: Harvester Press / Nueva York: Pantheon Books. Pág. 91.

Conclusión

El fenómeno de descontextualización en Facebook constituye, con certeza, una amenaza importante tanto para el derecho a la privacidad como para el derecho a la protección de datos. Los legisladores europeos tienen un punto de vista similar. De hecho, en su reciente opinión «sobre el establecimiento de redes sociales virtuales», el Grupo sobre Protección de Datos del artículo 29 señaló que una de sus preocupaciones clave era «la difusión y el uso de la información disponible en los sistemas de redes sociales para otros fines secundarios e involuntarios».[50] Para evitar la descontextualización de la información en los sistemas de redes sociales virtuales, el Grupo sobre la Protección de Datos aboga por una «seguridad robusta y configuraciones por defecto que salvaguarden la privacidad»[51] pero también quiere aumentar la responsabilidad de los usuarios imponiéndoles las obligaciones de un controlador de datos cuando se usa el sistema de redes sociales virtuales como «plataforma de colaboración para una asociación o empresa», donde el sistema de redes sociales virtuales se usa principalmente «como plataforma para impulsar objetivos comerciales, políticos o benéficos» , cuando el «acceso a la información del perfil se amplía más allá de los contactos seleccionados por el usuario» o cuando «los datos son codificables por los programas de búsqueda». Además, según el Grupo sobre Protección de Datos, «un gran número de contactos podría ser indicativo de que la excepción doméstica no es aplicable y, por tanto, de que el usuario sería considerado un controlador de datos».[52]

Dado que solo el 20% de los usuarios toca alguna vez sus ajustes de privacidad,[53] estoy convencido de que unos ajustes de privacidad por defecto más restrictivos constituirían una primera garantía contra la descontextualización. Dicho esto, albergo más dudas sobre la segunda propuesta del Grupo sobre Protección de Datos. De hecho, incrementar las responsabilidades de los usuarios con la esperanza de que se reducirá la descontextualización supone unos niveles elevados de conciencia y conocimiento en los usuarios. Sin embargo, la conciencia sobre los derechos y obligaciones en materia de protección de datos entre los ciudadanos parece seguir siendo bastante escasa. De hecho, según un reciente Eurobarómetro, «a pesar de los drásticos cambios tecnológicos producidos en las dos últimas décadas, el nivel de preocupación sobre la protección de datos prácticamente no ha cambiado».[54] Los mayores niveles de concienciación sobre la existencia de los derechos de protección de datos se encontraron en Polonia (43%), seguidos de Letonia (38%), Francia y Hungría (ambas con el 35%). Menos de uno de cada cinco ciudadanos de Suecia (16%) y Austria (18%) dijeron ser conscientes de las posibilidades legales con que cuentan para controlar el uso de sus propios datos personales.[55]

Por este motivo, y porque es importante para el Tribunal Europeo de Derechos Humanos «que se interprete y aplique de modo que su salvaguarda sea práctica y efectiva, en lugar de teórica e ilusoria»,[56] sinceramente creo que la protección de la privacidad y la protección de datos en Facebook no se debe centrar únicamente en las soluciones y penalizaciones para los individuos agraviados sino en el diseño de una arquitectura que rija los flujos de datos multi-contextuales en el sitio. Dada la importancia de la amenaza de la descontextualización, la arquitectura de Facebook debe estar diseñada de modo que evite cualquier interferencia tanto con el derecho a la privacidad como con la protección de datos, siempre que dicha interferencia no sea estrictamente necesaria en un estado democrático.

50. Grupo sobre Protección de Datos del artículo 29, opinión 5/2009 sobre el establecimiento de redes sociales virtuales, 12 de junio de 2009, pág. 3.
51. *Ibidem*.
52. *Ibidem*. Pág. 4.
53. Según el director de proyectos de Facebook, Chris Kelly, sólo el 20% de los usuarios modifica alguna vez sus ajustes de privacidad. Véase Randall STRESS (marzo, 2009). «When Everyone's a Friend, Is Anything Private?». *The New York Times*. Disponible en:
http://www.nytimes.com/2009/03/08/business/08digi.html
54. Véase RAPID PRESS RELEASE (abril, 2008). «Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection». *IP*/08/592.
55. Véase el EUROBARÓMETRO (febr., 2008). «Protección de datos en la Unión Europea: la percepción de los ciudadanos» (Informe analítico). Disponible en:
http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
56. Véase el TRIBUNAL EUROPEO DE DERECHOS HUMANOS (mayo, 1980). *Artico v. Italy*. Serie A n.º 37, págs. 15-16, § 33. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (2002). *Stafford v. the United Kingdom* [GC]. N.º 46295/99, § 68-IV.

Para lograr este objetivo, las autoridades europeas podrían incrementar la responsabilidad de los operadores de los sitios de establecimiento de redes sociales haciéndoles responder del diseño de sus sitios. Estos mecanismos ya existen en lo tocante al equipamiento de terminales en el contexto de las comunicaciones electrónicas. De hecho, según el artículo 14(3) de la Directiva 2002/58, «cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales». Del mismo modo, el artículo 3(3)(c) de la Directiva 1995/5 establece que «la Comisión podrá decidir que los aparatos dentro de ciertas clases de equipamiento o los aparatos de algún tipo en particular se construyan de modo que incorporen salvaguardas a fin de asegurar la protección de los datos personales y la privacidad del usuario y del suscriptor».

Con esto, las autoridades Europeas podrían imponer un contenido menos multi-contextual en los sistemas de establecimiento de redes sociales virtuales al requerir a los operadores de dichos sitios que diseñaran su arquitectura de acuerdo con las intenciones específicas de cada usuario. A modo de ejemplo, antes de que un usuario se registre en Facebook, se podría plantear una pregunta como «¿Con qué fin pretende usar Facebook?» con una lista de respuestas como «fin comercial», «fin político», «búsqueda de pareja», «relaciones laborales», «amistad en el mundo real», etc. Una vez determinado con mayor precisión el propósito del registro de cada usuario, Facebook debería obtener únicamente datos adecuados, relevantes y no excesivos con relación a ese fin. Si un usuario desea usar el servicio con múltiples propósitos, debería recomendarse el uso de múltiples cuentas. De un modo más general, los operadores de Facebook deberían considerar cuidadosamente «si pueden justificar el hecho de obligar a sus usuarios a actuar con su identidad real en lugar de con un pseudónimo».[57] En los casos en que el propósito específico del uso no requiere el nombre real, se debería recomendar el uso de pseudónimos.

La reconstrucción de lugares dentro de Facebook es una necesidad absoluta para que los usuarios evalúen qué normas contextuales de distribución y adecuación pueden esperar. Esta reclamación no sólo es útil para respetar la dividualidad de cada usuario en cuanto a su derecho a la protección de datos; de un modo más fundamental, es esencial para permitir a los usuarios construir su identidad como seres múltiples y relacionales y actuar, por ende, como seres humanos.

Cita recomendada

DUMORTIER, Franck (2009). «Facebook y los riesgos de la "descontextualización" de la información». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp>

ISSN 1699-8154

57. Grupo sobre Protección de Datos del artículo 29, opinión 5/2009 sobre el establecimiento de redes sociales virtuales, 12 de junio de 2009, pág. 11.

Sobre el autor

Franck Dumortier
Franck.dumortier@fundp.ac.be

Franck Dumortier es investigador senior en el CRID (Centro de Investigaciones en Informática y Derecho) y, desde 2005, asistente de derecho en las facultades universitarias de Notre Dame de la Paix en Namur. Sus estudios se centran particularmente en la interpretación del derecho con relación a la vida privada, en lo que se refiere al uso de las nuevas tecnologías, tales como la identificación por radiofrecuencia (RFID), la biometría, la vídeo-vigilancia o incluso las redes sociales virtuales.

Université de Namur
Centre de recherche informatique et droit (CRID)
Rempart de la Vierge 5,
B-5000 Namur, Bélgica

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

E-privacidad y redes sociales

Antoni Roig

Fecha de presentación: octubre de 2009
Fecha de aceptación: noviembre de 2009
Fecha de publicación: diciembre de 2009

Resumen
Los riesgos tecnológicos para la intimidad o la privacidad no se limitan a la problemática de las bases de datos. Las redes sociales, las etiquetas RFID, la computación ubicua y la robótica, por ejemplo, son otros ejemplos de riesgo para la privacidad. Las redes sociales también poseen valor económico y por ello cada vez se crean más ingenios que buscan la información personal de sus usuarios. En cambio, el estudio de la privacidad en las redes sociales es sólo una nueva área de estudio. A menudo, los expertos en tecnología de la información consideran la privacidad como un atributo cuantificable que se puede negociar y, probablemente, intercambiar entre individuos a cambio de ciertos beneficios. Nosotros creemos, en cambio, que la regulación debe favorecer las denominadas privacy enhancing technologies (PET) o tecnologías garantes de la privacidad. Esta garantía tecnológica de la privacidad es especialmente necesaria en las redes sociales. Los derechos fundamentales no pueden quedar reducidos sólo a opciones individuales que es preciso activar. Su componente de política pública podría estar garantizado si se incorporaran versiones favorables a la privacidad en el mismo diseño de las tecnologías de la información, como la privacidad por defecto. Otra vía interesante es conseguir que las empresas encuentren también un provecho económico en la previsión de tecnología garante de la privacidad

Palabras clave
redes sociales, *privacy-enhancing technologies*, privacidad, e-privacidad, análisis de redes sociales, privacidad en el diseño

Tema
Protección de datos

e-Privacy and Social Networks

Abstract
The technological risks for privacy and anonymity are not limited to the problems of databases. Social networks, RFID tags, ubiquitous data processing and robotics, for example, are other examples of risk. Social networks have an economic value and search engines increasingly try to access their users' personal information. In contrast, the study of privacy in social networks is a new area. Experts in information technology generally consider privacy as a quantifiable attribute which can be negotiated and probably exchanged between individuals for certain benefits. We believe, on the other hand, that regulation should favour the so-called Privacy Enhancing Technologies (PET) to guarantee privacy, and that these are particularly necessary

in social networks. Fundamental rights cannot be reduced to individual options which need to be activated. The public component of public policy could be guaranteed if versions favourable to privacy were incorporated in the design of information technologies themselves, such as privacy by default. Another way may be for businesses to see economic benefits in planning technological measures guaranteeing privacy.

Keywords
social networks, privacy-enhancing technologies, privacy, e-privacy, analysis of social networks, privacy in design

Subject
Data protection

1. La reducción de la privacidad en la protección de datos personales en bases de datos automatizadas

En España, como en el resto de Europa, la e-privacidad o privacidad electrónica ha quedado, en buena medida, reducida al derecho a la protección de datos personales en bases de datos automatizadas. Veamos rápidamente el proceso.[1] El punto de partida en nuestro país es el artículo 18.4 CE, en el que se puede leer: «La ley limitará el uso de la informática con el fin de garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Pues bien, en un primer momento, hasta el año 2000, el Tribunal Constitucional no reconocerá un derecho autónomo a la protección de datos. La jurisprudencia constitucional, basándose en el *leading case* de la STC 254/1993, partirá del derecho a la intimidad (artículo 18.1 CE), al que añadirá una vertiente informática. Esta construcción era claramente artificial, ya que el derecho a la intimidad es un derecho de libertad clásico que sólo pretende preservar de los poderes públicos una esfera personal de libertad. La abstención de actuación del Estado es suficiente para garantizar el derecho. En cambio, el derecho a la protección de datos debe ser garantizado junto a una serie de facultades de actuación por parte de la persona y, a menudo, contra la actuación de otro particular, y no sólo de los poderes públicos. Hasta la STC 292/2000 el Tribunal Constitucional no configurará el derecho a la protección de datos con más precisión, y de manera separada del derecho a la intimidad.

Pero ¿qué efectos tiene esta evolución jurisprudencial sobre la privacidad, en general, y sobre la e-privacidad, en particular? Resumidamente, la decisión sobre el artículo 18.4 CE ha reducido los efectos de las nuevas tecnologías sobre los derechos fundamentales en la problemática de las bases de datos. Para entenderlo, es preciso saber que la Constitución española, a diferencia de la portuguesa o la americana, por ejemplo, no contiene ninguna cláusula de actualización de derechos fundamentales. Por lo tanto, los posibles nuevos derechos que aparezcan como consecuencia de la extensión de las nuevas tecnologías de la información y la comunicación no pueden ser descubiertos autónomamente por el Tribunal Constitucional. El artículo 18.4 CE es la única referencia a la informática en la Constitución de 1978, anterior al crecimiento exponencial de Internet en los años noventa. Por lo tanto, si hemos acotado los problemas informáticos al derecho a la protección de datos, las otras garantías deberán provenir de los derechos fundamentales tradicionales: la libertad de expresión y de información, el derecho al honor, a la intimidad personal y familiar y a la propia imagen, y el derecho al secreto de las comunicaciones.

1. Para más detalles, podéis leer el trabajo: ROIG, Antoni (2002). «La protecció de les bases de dades personals. Análisi de la jurisprudencia del Tribunal Constitucional». *Revista Jurídica de Catalunya*, n.º 2, pág. 141-156.

En nuestra opinión, desde el año 2000 estamos en una etapa transitoria, en la que se ha resuelto la precisa delimitación del derecho a la protección de datos, pero en la que quedan por resolver otras posibles manifestaciones de restricciones tecnológicas de derechos fundamentales. Cuando aparezca una pretensión de garantizar un derecho que no se pueda reconducir claramente a la intimidad, a la libertad de expresión y al secreto de las comunicaciones, será necesario reabrir el debate sobre el artículo 18.4 CE, o sobre la cláusula de actualización de derechos, quizá a partir del derecho a la dignidad humana, como proponía el magistrado Jiménez de Parga en su voto particular en la STC 290/2000. La e-privacidad quizá será tan difícil de proteger desde el derecho tradicional a la intimidad como lo ha sido el derecho a la protección de datos. Téngase en cuenta, por ejemplo, que el derecho a la intimidad está pensado para posibles infracciones por parte de poderes públicos. En cambio, la privacidad en las redes sociales la ponen en peligro, preferentemente los particulares que ofrecen este servicio en Internet. La posibilidad de infracción de derechos fundamentales por particulares ya ha sido reconocida en un ámbito tan importante como el laboral, en el que los trabajadores no renuncian a sus derechos fundamentales cuando entran en la empresa.

La posición dominante en Europa, como se ha indicado, la tiene la Directiva 95/46/CE, de Protección de Datos.[2] Parece que los esfuerzos por obtener un estándar internacional sobre privacidad en las redes sociales se basarán en principios generales de la protección de datos personales. A pesar de la importancia de este eventual reconocimiento internacional, pensamos que no se evitarán así todos los riesgos tecnológicos para la privacidad. Precisamente, en las redes sociales no todos los riesgos provienen de posibles bases de datos personales, como veremos.

2. Hacia una regulación estándar internacional de principios basados en la protección de datos

No es extraño que el marco regulador para la privacidad en las redes sociales se base en principios generales de protección de datos. De hecho, incluso la Administración Obama parece considerar conveniente el modelo de la Directiva europea de Protección de Datos, frente a la miscelánea legislativa y a los códigos de conducta voluntarios que menudean en Estados Unidos. Así pues, el marco regulador lo constituirán las leyes nacionales de protección de datos que incorpora la Directiva europea. Si se desea tener un conocimiento detallado y actualizado de la interpretación de la normativa de protección de datos, es necesario acudir a los dictámenes y estudios jurídicos de la Agencia de protección de datos. En un ámbito internacional, el grupo del artículo 29 de la Directiva europea reúne a las principales agencias de protección de datos europeos y emite informes de gran interés y novedad. Ya disponemos de un marco general de informes que permite anticipar el contenido principal de los principios reguladores del futuro estándar internacional.

Así, en primer lugar, el Memorándum de Roma del 2008 es el marco principal de referencia sobre redes sociales y privacidad.[3] El informe intenta explicar por qué hay tan poca regulación sobre la publicación de datos personales a iniciativa de los propios particulares. La explicación sería doble: no ha sido ésta una cuestión relevante fuera de la Red, y sólo ha empezado a destacar en ésta a partir de la aparición de las redes sociales; otra consideración sería sociológica, en este caso la existencia de una nueva generación, los denominados «digital natives» o nativos digitales, que se caracterizarían por sentirse cómodos a pesar de publicar detalles, algunas veces incluso íntimos, de su vida

2. *Diario Oficial*, n.º L281 de 23/11/1995, pág. 31.
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
3. INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2008). «Report and Guidance on Privacy in Social Network Services (Memorandum de Roma)». En: *43.ª reunión* (3-4 de marzo del 2008: Roma) [informe en línea]. Informe n.º 675.36.5. IWGDPT.
http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

en la Red. Las recomendaciones del Memorándum de Roma a los legisladores serían:

- Introducir la opción de un derecho al uso de seudónimos.
- Asegurarse de que los proveedores de servicios sean honestos y transparentes en cuanto a la información requerida por el servicio básico. El consentimiento de los menores también demandará una solución específica.
- Obligación de notificación de cualquier riesgo para los datos personales que se haya podido producir.
- Posiblemente será necesario atribuir más responsabilidad a los proveedores sobre los datos personales en la Red.
- Introducir en la escuela la temática de la privacidad y de las herramientas protectoras.

En el año 2008 también se adoptó una resolución sobre la protección de la privacidad en los servicios de las redes sociales por parte de las agencias de protección de datos.[4] De todas maneras, nos parece más relevante la Posición número 1 de ENISA del año 2007 (European Network and Information Security Agency).[5] Algunas de las recomendaciones que parecen más destacadas son:

- Las redes sociales deberían usar, siempre que sea posible, una información adaptada al contexto, con el objetivo de educar en tiempo real.
- Las campañas de concienciación deberían ir dirigidas también a los programadores de software, con el fin de favorecer prácticas y políticas de empresa que respeten la privacidad.
- Es necesario realizar un estudio atento de la regulación que pueda aplicarse a las redes y revisar o dar respuesta adecuada, como mínimo, a las siguientes cuestiones:
  - ¿Qué sucede con el contenido de un usuario que el proveedor de servicios borra porque lo considera *spam*?
  - ¿Qué sucede con las etiquetas o comentarios en las imágenes (*image-tagging*) colocados por terceros?
  - ¿Quién es responsable de los problemas de seguridad derivados de la actividad de los usuarios?
  - ¿Cómo se deberían comunicar a los usuarios las políticas de privacidad de terceros incluidos en la Red?
  - ¿Qué es un dato personal en una red social?
  - ¿Cuál es la posición legal del que suplanta un perfil?
  - ¿Se deberían proteger algunos datos de menores, como la localización?
- Se debería informar a los usuarios de lo que se hace con sus datos antes y después de cerrar la cuenta.
- El fenómeno de las redes se debería tratar de manera controlada y transparente, sin prohibir o desaconsejar, con campañas dirigidas a los menores, a los profesores y a los padres.

El tercer documento relevante es el *Working Paper* (n.º 163) del grupo de trabajo del artículo 29, sobre redes en línea, del 12 de junio del 2009.[6] Este documento avanza en la aplicación de la Directiva de Bases de Datos Personales en el ámbito de las redes sociales.

- Obligación de los proveedores de cumplir con la Directiva de protección de datos, e incluso la Directiva de e-privacidad, si ofrecen servicios de comunicaciones electrónicas.
- Obligación de los proveedores de informar de su identidad e indicar las diferentes finalidades con las que se tratan los datos personales de los usuarios.
- Se recomienda que sólo se puedan colgar imágenes e información de terceros con el consentimiento de los individuos en cuestión.

4. Adoptada en la XXXII Conferencia Internacional de Agencias de Protección de Datos y Privacidad en Estrasburgo, el 17 de octubre del 2008.
http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf.
5. HOGBEN, G. (ed.) (octubre, 2007). «Security Issues and Recommendations for Online Social Networks». *Enisa Position Paper*, n.º 1.
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
6. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea* [informe en línea].
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf

- Los proveedores tendrían la obligación de advertir del derecho a la privacidad de los terceros.
- En el caso de datos sensibles, el consentimiento debería ser explícito, a menos que fuera un dato público. Si la red social incluye algún dato sensible en el perfil, debería hacer constar que es voluntario contestar. Las imágenes no serán un dato sensible, a menos que claramente sean usadas para revelar datos sensibles de los individuos.
- En cuanto a los datos de terceros, si los responsables de la Red informan a ese tercer no usuario acerca de la existencia de datos personales sobre él, un hipotético correo electrónico en el que se le invitara a ser usuario de la aquélla también podría vulnerar la prohibición del artículo 13.4 de la Directiva de e-privacidad, cuando se refiere al envío de mensajes electrónicos no solicitados para finalidades comerciales.
- Los socios terceros de la Red, que ofrecen servicios adicionales y que utilizan los datos personales en aquélla, deberían estar advertidos de que deben cumplir también las directivas mencionadas.

Incluso encontramos aquí una novedad interesante, más latente en las recomendaciones anteriores: la herramienta preferida para garantizar la privacidad es una buena seguridad y un funcionamiento garante de la privacidad (*privacy-friendly*) por defecto.

- Las redes sociales deberían prever estas características favorables a la privacidad sin coste añadido y restringiendo el acceso a los contactos seleccionados por el propio usuario. Cuando el acceso al perfil de información va más allá de los contactos seleccionados por el usuario, por ejemplo a todos los usuarios de la red social, o cuando el usuario debe aceptar contactos, independientemente de la relación que tengan con él, o si el dato no se puede indexar mediante un motor de búsqueda, nos encontraríamos con un acceso equivalente a público. Esto podría suponer la aplicación al usuario de la Directiva de protección de datos, por la que se le asimilaría a las responsabilidades que adquiere un responsable de una base de datos. Puesto que no se trataría ya de un ámbito doméstico, sino público, incluso la libertad de expresión debería ser matizada con el debido respeto al derecho a la privacidad. En esta línea, puesto que no concurre la excepción de uso doméstico, sería necesario proteger los derechos de terceros, sobre todo con relación a sus datos sensibles.
- El acceso restringido a los perfiles no debería ser posible con motores de búsqueda internos, con parámetros como la edad o la dirección. Además, las decisiones para extender el acceso no deberían estar implícitas.

Finalmente, destacamos la solución propuesta para el caso especial de los menores: la inclusión de medidas tecnológicas o *privacy enhancing technologies*:

- Educación escolar.
- No solicitar datos sensibles en el formulario de suscripción; no dirigir el marketing directo a los menores; obtener el consentimiento previo de los padres o tutores; y separar la comunidad de menores de la de adultos.
- Desarrollar *privacy enhancing technologies* (PET), por ejemplo, avisos en forma de *pop-up* o ventanas en ciertos momentos determinantes, o software de verificación de la edad.
- Código de conducta de los proveedores.

3. Riesgos no cubiertos por la protección de datos: el análisis de las redes sociales

3.1. Análisis de redes sociales (*social network analysis*)

El interés económico que genera la información personal contenida en las redes sociales ha provocado que crezcan proyectos comerciales a partir de la dirección de la Red, con socios terceros, y que aparezcan cada vez más herramientas de análisis de redes para particulares no asociados a la Red. Inicialmente, eran herramientas matemáticas sencillas ligadas a la teoría de *grafos* y a técnicas básicas sociológicas. En la actualidad se han vuelto cada vez más complejas, e incluyen interacción social y sistemas de reputación. Sus usuarios ya no son sólo los sociólogos o los estudiosos de las comunidades en línea, sino también particulares o profesionales que buscan colaboradores. Herramientas como VisoLink están, pues, centradas en el usuario y plantean retos para la privacidad.[7] Actualmente, las redes sirven tanto para el entretenimiento como para los profesionales, que participan en ellas. En el campo de la ciencia médica, por ejemplo, es vital poder intercambiar información sobre casos clínicos y metodologías en el

tiempo más corto posible, así como crear bases de datos históricas.[8]

Pero el riesgo no proviene sólo de motores de búsqueda externos de alcance cada vez más universal e incluso personalizado, el peligro para la privacidad radica también en la captura de información personal que el usuario involuntariamente ha puesto en la Red. Aquí no existe ninguna base de datos, ni siquiera una fuente estructurada o un dato personal explícito. A pesar de todo, una investigación llevada a cabo en una red social concreta ha revelado que el nombre del 72% de los usuarios y su nombre completo en un 30% de los casos podían deducirse fácilmente de los perfiles con técnicas estadísticas y heurísticas. Asimismo, la edad del 15% de los usuarios y, al menos, una escuela del 42% de los usuarios podían también deducirse de los datos colgados en la red social.[9]

3.2. La web 3.0, con los servicios de la web semántica, aumenta este riesgo para la privacidad

De hecho, con la creciente implantación de la tecnología de la web semántica, en la que los motores de búsqueda ya no se limitarán a las palabras clave sino también a sus significados, estos riesgos para la privacidad todavía serán más importantes. De hecho, las aplicaciones de web semántica añadirán al análisis de las redes sociales la posibilidad de extraer ontologías, es decir, mapas de significado, de las páginas web. De este modo, se obtendrá no sólo la ontología de conocimiento técnico elaborada por un experto, sino también una nueva estructura de significado basada en las relaciones en la comunidad en red, una semántica emergente.[10] La propia noción de dato personal queda aquí mortalmente debilitada, ya que la tecnología permite extraer datos personales, cada vez con más precisión y complejidad, de contextos desestructurados y sin capacidad, aparentemente, para identificar a nadie. La inclusión de la IP en el grupo de los datos personales sorprendió en su momento. Ahora nos enfrentamos al riesgo de que la capacidad de transformar en personal (identificable) un conjunto de datos aparentemente inocuos alcance niveles todavía más inverosímiles.

4. Las *privacy enhancing technologies* (PET) o tecnologías garantes de la privacidad

Un jurista suele considerar la tecnología como un riesgo para la privacidad. Esto puede ser efectivamente así, como se ha indicado antes. Ahora bien, estamos llegando a un nivel de posibilidades técnicas tan alto que se hace difícil incluso defender algunos derechos, como el de la privacidad, sin recurrir a contramedidas técnicas. Ésta es la idea de las PET o técnicas garantes: no sólo la tecnología no es el riesgo aquí, sino que también puede ser, si se dan las circunstancias propicias, una manera de proteger efectivamente el derecho. Los principios o recomendaciones a los legisladores apuntan tímidamente a esta posibilidad. Los ingenieros, a base de subvenciones públicas en proyectos de investigación europeos, ya han empezado a proponer prototipos que pronto serán adoptados por las redes sociales.[11] Vemos algunas de las posibilidades y capacidades de estos ingenios protectores.

4.1. La protección tecnológica contra los motores de búsqueda o minería de datos: el *privacy-preserving data mining* (P2DM)

La protección tecnológica de la privacidad es un área nueva, con menos de 10 años y con un planteamiento todavía muy teórico. En cambio, el *privacy-preserving data mining* (P2DM) es la excepción. El objetivo del P2DM es evitar, en la medida de lo posible, que se haga pública

7. FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». En: G. WANG [*et al.*] (eds.). *Lecture Notes in Artificial Intelligence*, n.º 5009, pág. 668-675.
8. VERAGO, R; CEDRATI, F. C.; D'ALESSI, F; ZANETTE, A. (2008). «Eye Knowledge Network: A Social Network for the Eye Care Community». En: M. D. LYTRAS [*et al.*] (eds.). *WSKS 2008. Lecture Notes in Artificial Intelligence*, n.º 5288, pág. 22-30.
9. LAM, I.-F.; CHEN, K.-T.; CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». En: K. MATSUURA; E. FUJISAKI (eds.). *IWSEC* (2008). *Lecture Notes in Computer Science*, n.º 5312, pág. 167-183.
10. MIKA, P. (2007), *Social Networks and the Semantic Web*. Nueva York: Springer.
11. Workshop on Privacy and Protection in Web-based Social Networks, 8 de junio del 2009, en el marco de la International Conference on Artificial Intelligence and Law. Barcelona, en prensa.

información personal de los usuarios de la Red cuando se analicen sus datos con finalidades estadísticas. Una herramienta de protección de la privacidad en las redes debe tener en cuenta no sólo los atributos de los usuarios, sino también sus relaciones.[12]

4.2. La protección tecnológica del acceso, de la identificación y de los sistemas de reputación

Las redes se basan en la confianza. Normalmente, la confianza se obtiene con el conocimiento del otro. Esto provoca que se considere habitualmente que cuanta más confianza hay, más datos personales identificables (PII, en inglés) del otro se desea tener y, por lo tanto, más riesgo para la privacidad.

Para romper esta lógica perversa, se ha pensado en primer lugar en mecanismos de autoidentificación o de reconocimiento, sin identificación. La idea es tener, al mismo tiempo, privacidad y confianza. Un modo de lograrlo es mediante el uso de seudónimos, que es una de las recomendaciones a los legisladores más habituales por parte de las agencias de protección de datos y grupos de expertos. Ahora bien, ésta tampoco es una solución definitiva: el análisis de la red social y la minería de datos pueden conseguir asociar estadísticamente un seudónimo a un usuario real. Por ello, los expertos recomiendan el uso de múltiples seudónimos. Existen soluciones técnicas para evitar el mal uso de los múltiples seudónimos.[13] En la misma línea, el proyecto europeo PRIME (Privacy and Identity Management for Europe) emplea credenciales privadas. Estas credenciales sirven de prueba de las autorizaciones, por ejemplo, ser mayor de edad, sin identificar al usuario. Sólo en caso de mal uso el anonimato podrá ser revocado.[14]

Como hemos indicado, las redes adoptan sistemas de reputación para garantizar la confianza. Ahora bien, los actuales sistemas de reputación generan perfiles del usuario que incluyen todos los contextos en los que éste ha estado interviniendo. Eso es frecuente en las redes de compraventa electrónica, en las que el tiempo, la frecuencia de la participación, la evaluación y el interés por ciertos productos pueden ser controlados. Además, los actores económicos suelen tener su seudónimo vinculado a un nombre real, lo que provoca que el perfil sea plenamente identificado. Otro riesgo en los sistemas de reputación se debe a los diferentes tipos de relaciones entre usuarios, como «amigo de». En el año 2006, miles de usuarios de Facebook protestaron por una utilidad denominada News Feed, que daba cuenta de la última información personal de los usuarios catalogados como amigos.[15] Para detener la avalancha de críticas, Facebook permitió a los usuarios disponer de algunas preferencias de privacidad. Más adelante, en noviembre del 2007, otro servicio de Facebook generó controversia: Beacon.[16] Beacon forma parte del sistema de alertas de Facebook, que sigue las actividades de los usuarios en la navegación por las páginas web de sus *partners*. Esta navegación era puesta a disposición de los amigos del usuario sin su consentimiento. De nuevo, las redes sociales han reaccionado ante las críticas, y han ofrecido a los usuarios mecanismos opcionales que permiten o no el acceso a su información personal (www.facebook.com, http://videntity.org).

Ahora bien, son necesarias estrategias más flexibles que permitan al usuario definir su política privada personal. La idea es que los usuarios indiquen quiénes están autorizados a acceder a su página personal, incluso si no son usuarios conectados con una relación de amistad.[17] Una opción es mediante un control de acceso por parte del

12. WANG, D.-W.; LIAU, C.-L.; HSU, T.-S. (2006). «A GrC-Based Approach to Social Network Data Protection». En: S. GRECO [*et al.*] (eds.). *RSCTC 2006. Lecture Notes in Artificial Intelligence*, n.º 4259, pág. 438-447.
13. SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». En: J. GOLBECK (ed.). *Computing with Social Trust*, Londres: Springer. Human-Computer Interaction Series.
14. HANSEN, M. (2008). «Marrying Transparency Tools with User-Controlled Identity Management». En: S. FISCHER-HÜBNER; P. DUQUENOY; A. ZUCCATO; L. MARTUCCI. *The Future of Identity in the Information Society*. IFIP International Federation for Information Processing. Vol. 262, pág. 199-200. Boston: Springer.
15. CHEN, L. (octubre, 2006). «Facebook's feeds cause privacy concerns. The amherst student». http://halogen.note.amherst.edu/astudent/2006-2007/issue02/news/01.html
16. BERTEAU, S. (2007). «Facebook's misrepresentation of beacon threats to privacy: Tracking users who opt out or are not logged in». http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-trackingusers-who-opt-out-or-are-not-logged-in.aspx

propio usuario,[18] o mediante la colaboración de un grupo de usuarios seleccionados, o sin un nódulo central.[19] Dicho esto, el control de acceso no es la única manera de preservar la privacidad en las redes sociales. Es necesario plantear otros sistemas de reputación garantes de la privacidad desde una óptica más general.

4.3. Sistemas de reputación garantes de la privacidad no basados en el acceso

Ya hemos indicado que las recomendaciones de las agencias de protección de datos, en el sentido de usar seudónimos, deberían traducirse en una multiplicidad de seudónimos. También hemos señalado que es necesario evitar el mal uso de éstos. Ahora debemos añadir que se puede obtener un sistema de reputación fiable con valoraciones de los seudónimos en diferentes contextos. Este esquema ha sido, incluso, propuesto para redes de P2P con seudónimos.[20] Se dispone de unos puntos de reputación (*e-cash*). Un usuario honesto puede cambiar su seudónimo conservando su reputación. En cambio, un usuario deshonesto no podrá borrar su cuenta de puntos, ni siquiera cambiando de seudónimo.

4.4. Tecnología para la transparencia, el contexto y la finalidad

Las tecnologías tradicionales garantes de la privacidad han buscado la anonimización, la seudoanonimización y la autenticación. Parece existir una tendencia que favorece actualmente las PET más centradas en la transparencia. En todo caso, son estrategias complementarias. Seguramente, la implantación progresiva de la normativa europea sobre protección de datos, muy centrada en el control de la información y en la finalidad, puede explicar, cuando menos, parcialmente, este nuevo enfoque.

Las tecnologías de la transparencia deben garantizar que el flujo de información sea visible y deje rastro. Y se pretende que lo hagan de una manera amplia, que afecten tanto a las políticas de privacidad como al procesamiento de los datos, a los servicios ofrecidos, al software utilizado, a los colaboradores y a la confianza, así como a posibles problemas de seguridad. Las herramientas de transparencia, por sí solas, no solucionan los riesgos para la privacidad. Sólo su combinación con la gestión de la identidad y los sistemas de reputación puede ofrecer garantías para la privacidad.

Una posibilidad extrema es la de las TET (*transparency enhancing technologies*), que pretende anticipar un posible perfil que se pueda deducir de los datos de un particular. La idea central es disponer de suficiente información para ser capaz de construir un perfil contrario a lo que se deduce de la información disponible. El uso más habitual de la tecnología de la transparencia, sin embargo, es poder saber en todo momento qué dato personal se ha proporcionado al sistema, con el fin de acceder a él, alterarlo o borrarlo. En el proyecto europeo PRIME, el buscador de datos o Data Track cumple esta función. Antes de dar información personal se puede consultar la actividad de los colaboradores y la política de privacidad. Esta información sirve también para pedir a los responsables de los datos si han actuado correctamente o para investigar riesgos detectados en anteriores utilizaciones del buscador de datos.

Conclusiones

La protección de la privacidad en las redes sociales no es la adecuada. Hay varias razones que coinciden en esta situación delicada:

- El marco regulador es inexistente o muy limitado. Sólo la regulación sobre la protección de las bases de datos

17. CARMINATI B.; FERRARI, E. (2008). «Privacy-Aware Collaborative Access Control in Web-Based Social Networks». En: V. ATLURI (ed.). *Lecture Notes in Computer Science*, n.º 5094, pág. 81-96.
18. CARMINATI B.; FERRARI, E.; PEREGO, A. (2007). «Private relationships in social networks». En: *ICDE 2007 Workshops Proceedings*. Los Alamitos: IEEE CS Press. Pág. 163-171.
19. DOMINGO-FERRER, J. (2007). «A Public-Key Protocol for Social Networks with Private Relationships». En: V. TORRA, Y. NARUKAWA; Y. YOSHIDA (eds.). *MDAI 2007. Lecture Notes in Artificial Intelligence*, n.º 4617, pág. 373-379.
20. ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». En: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008. Lecture Notes in Computer Science*, n.º 5134, pág. 202-218.

personales configura un cuerpo destacado. Ahora bien, su plena vigencia se centra en los países europeos. Existe, no obstante, una tarea muy notable de las agencias de protección de datos, y de los grupos de trabajo próximos a éstas, que va concretando medidas y recomendaciones útiles. En este sentido, se está intentando llegar a un estándar internacional de privacidad en las redes sociales que podría resultar un primer marco regulador de referencia en la materia. Ahora bien, la reducción de toda la problemática a la protección de las bases de datos excluye aspectos relevantes de la protección de la privacidad en las redes sociales que sería preciso no olvidar.

- La tecnología de protección de la privacidad aparece por primera vez, tímidamente, en algunas recomendaciones. La fragilidad es doble: por un lado, existe una fundamentación jurídica de la tecnología como garante de derechos. Más bien al contrario, la tecnología es vista como fuente de riesgos para los derechos. Una posible fundamentación podría derivar del principio de proporcionalidad, que rige las limitaciones de derechos. En resumen, la necesidad de una restricción de derechos se valora por la imposibilidad de llevar a cabo una finalidad legítima, como podría ser la gestión de una red social, con una menor afectación a los derechos. Pues bien, si las PET o tecnologías garantes de la privacidad fueran de alcance público, se podrían cuestionar las restricciones de la privacidad como medidas desproporcionadas, por innecesarias. Por otro lado, las PET tienen muchas dificultades para pasar del aspecto teórico de los proyectos europeos, que es en el que aparecen, al posterior desarrollo y aplicación comercial. No parece existir impulso público ni conciencia particular de esta delicada situación y, por ahora, son considerados por la industria como un gasto extra no impuesto por ninguna ley, ni sancionado por ninguna agencia.
- Las redes sociales son un campo especialmente vulnerable para la privacidad. Pero no son el único: la computación ubicua, las etiquetas RFID y la robótica, según nuestros limitados conocimientos, son también retos muy difíciles. Una posible aproximación, más anglosajona, consiste en hacer que la industria tenga interés económico en desarrollar herramientas que incorporen una versión «amiga de la privacidad». El interés de esta propuesta consiste en que las soluciones son más sencillas y más baratas si se incorporan ya en el diseño del sistema o programa que si se intenta añadir *a posteriori* un «paquete» adicional de PET. Quizá por ello, las propias PET van incorporando otras opciones además de las tradicionales basadas en el anonimato, los seudónimos y las autenticaciones. Parece dibujarse, no obstante, un riesgo: la negociación de las facultades o derechos entre el usuario y la red social, o entre usuarios, a cambio de beneficios, transforma los derechos fundamentales en opciones individuales. Tal vez la privacidad puede acabar de diluirse en este mercado de intercambios o de concesiones. Por esta razón queremos destacar el dictamen, en el marco de las etiquetas RFID, del supervisor europeo de protección de datos que, por desgracia, todavía no parece haber llegado a las propuestas de las agencias sobre redes sociales: la previsión de las medidas tecnológicas garantes de la privacidad en el mismo momento del diseño de la herramienta.[21] Éste es un reto no sólo para los ingenieros de las PET, que deberán pensar «en tiempo real» y en el contexto específico de un producto comercial; también lo es para el derecho, si no nos queremos quedar, en el mejor de los casos, con un listado de principios generales. La previsión de estándares técnicos protectores de la privacidad podría ser la última oportunidad para la regulación, entendida ésta como una competición entre los intereses comerciales particulares y los intereses generales, como es el caso de la privacidad. La redefinición de la privacidad se realizará, presumiblemente, no en grandes definiciones, sino en pequeñas y constantes redefiniciones de técnicas garantes en ámbitos como las redes sociales. Si no estamos atentos, el derecho a la privacidad puede acabar siendo sólo un «derecho ficción».

21. Dictamen del Supervisor Europeo de Protección de Datos relativo a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «La identificación por radiofrecuencia (RFID) en Europa: Pasos hacia un marco político», documento COM (2007) 96, (2008/C101/01), donde habla de la necesidad «de intimidad mediante el diseño».

Referencias

ANDROULAKI, E.; CHOI, S. G.; BELLOVIN, S. M.; MALKIN, T. «Reputation Systems for Anonymous Networks». En: N. BORISOV; I. GOLDBERG (eds.). *PETS 2008, Lecture Notes in Computer Science*. N.º 5134, pág. 202-218.

BERTEAU, S. (2007). «Facebook's misrepresentation of beacon threats to privacy: Tracking users who opt out or are not logged in». ‹http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-trackingusers-who-opt-out-or-are-not-logged-in.aspx›

CARMINATI B.; FERRARI, E. (2008). «Privacy-Aware Collaborative Access Control in Web-Based Social Networks». En: V. ATLURI (ed.). *Lecture Notes in Computer Science*. N.º 5094, pág. 81-96.

CARMINATI B.; FERRARI, E.; PEREGO, A. (2007). «Private relationships in social networks». En: *ICDE 2007 Workshops Proceedings*. Los Alamitos: IEEE CS Press. Pág. 163-171.

CHEN, L. (octubre, 2006). «Facebook's feeds cause privacy concerns. The amherst student». ‹http://halogen.note.amherst.edu/astudent/2006-2007/issue02/news/01.html›

DOMINGO-FERRER, J. (2007). «A Public-Key Protocol for Social Networks with Private Relationships». En: V. TORRA, Y. NARUKAWA; Y. YOSHIDA (eds.). *MDAI 2007*, *Lecture Notes in Artificial Intelligence*. N.º 4617, pág. 373-379.

FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». En: G. WANG [*et al.*] (eds.). *Lecture Notes in Artificial Intelligence*. N.º 5009, pág. 668-675.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2009). *Dictamen 5/2009 sobre las redes sociales en línea*. [informe en línea]. ‹http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf›

HANSEN, M. (2008). «Marrying Transparency Tools with User-Controlled Identity Management». En: S. FISCHER-HÜBNER; P. DUQUENOY; A. ZUCCATO; L. MARTUCCI. *The Future of Identity in the Information Society*. IFIP International Federation for Information Processing. Vol. 262, pág. 199-200. Boston: Springer

HOGBEN, G. (ed.) (octubre, 2007). «Security Issues and Recommendations for Online Social Networks». *Enisa Position Paper*. N.º 1. ‹http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf›

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2008). «Report and Guidance on Privacy in Social Network Services (Memorandum de Roma)». En: *43.ª reunión* (3-4 de marzo del 2008: Roma) [informe en línea]. Informe n.º 675.36.5. IWGDPT. ‹http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491›

LAM, I.-F., CHEN, K.-T. y CHEN, L.-J. (2008). «Involuntary Information Leakage in Social Network Services». En: K. MATSUURA; E. FUJISAKI (eds.). IWSEC (2008). *Lecture Notes in Computer Science*. N.º 5312, pág. 167-183.

MIKA, P. (2007). *Social Networks and the Semantic Web*. Nueva York: Springer.

SEIGNEUR, J. M. (2009). «Social Trust of Virtual Identities». En: J. GOLBECK (ed.). *Computing with Social Trust*. Londres: Springer. Human-Computer Interaction Series.

VERAGO, R; CEDRATI, F. C.; D'ALESSI, F; ZANETTE, A. (2008). «Eye Knowledge Network: A Social Network for the Eye Care Community». En: M. D. LYTRAS [*et al.*] (eds.). *WSKS 2008*, *Lecture Notes in Artificial Intelligence*. N.º. 5288, pág. 22-30.

WANG, D.-W.; LIAU, C.-L.; HSU, T.-S. (2006). «A GrC-Based Approach to Social Network Data Protection». En: S. GRECO [*et al.*] (eds.). *RSCTC 2006*, *Lecture Notes in Artificial Intelligence*. N.º 4259, pág. 438-447.

Cita recomendada

ROIG, Antoni (2009). «E-privacidad y redes sociales». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_roig/n9_roig_esp›

ISSN 1699-8154

Sobre el autor

Antoni Roig
antoni.roig@uab.cat

El Dr. Antoni Roig es profesor de Derecho constitucional en la Facultad de Derecho de la UAB. Ha sido investigador en proyectos nacionales y europeos. Cuenta con publicaciones en las áreas de fuentes del derecho, derecho europeo, bases de datos, tecnología y libertad de expresión y privacidad de ciudadanos y trabajadores. Sus últimas publicaciones se han centrado en la privacidad y el gobierno electrónico.

Cuenta con un doctorado en Derecho por la UAB y ha realizado estudios post-doctorales en las Universidades Cattolica di Milano (Milán, 1996-1997) y Università degli Studi di Firenze (Florencia, 1997). En la actualidad, participa en un curso de ingeniería técnica informática en la Universitat Oberta de Catalunya.

IDT, Instituto de Derecho y Tecnología
Universidad Autónoma de Barcelona
08193 Bellaterra (Barcelona), España

IDP. Revista de Internet, Derecho y Política es una publicación electrónica semestral impulsada por los Estudios de Derecho y Ciencia Política de la UOC, que tiene como objetivo la comunicación y divulgación científica de trabajos de análisis e investigación sobre los retos y cuestiones que las tecnologías de la información y la comunicación plantean con respecto al derecho y la ciencia política.

IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA. N.º 9 (2009)

EDITA: Àrea de Comunicació. Publicacions a Internet. **DIRECCIÓN:** Eric Hauck. **DIRECTOR DE PUBLICACIONES EN INTERNET:** Lluís Rius **COORDINACIÓN EDITORIAL:** Maria Boixadera. **ASISTENTE DE EDICIÓN:** Margarita Perelló. **CORRECCIÓN Y TRADUCCIÓN DE TEXTOS:** Clara Ortega, Nita Sáenz (Eureca Media, SL), Shirley Burgess y Michael van Laake (inglés). **MAQUETACIÓN:** Maria Abad (Eureca Media, SL). **DISEÑO:** Elogia y Grafime. **ISSN:** 1699-8154. **DEPÓSITO LEGAL:** B-29.619-2005. **DIRECCIÓN POSTAL:** Universitat Oberta de Catalunya. Avda. Tibidabo, n.º 39-43. 08035 Barcelona. **DIRECCIÓN ELECTRÓNICA:** idp@uoc.edu. **WEB IDP:** http://idp.uoc.edu/

UOC
Universitat Oberta de Catalunya
www.uoc.edu