El *big data* en el marco del Reglamento General de Protección de Datos

PID_00251298

Alessandro Mantelero

Universitat Oberta de Catalunya

Índice

Introducción

Cuando en el año 2012 el nuevo Reglamento sobre protección de datos empezó a dar sus primeros pasos en el proceso que condujo a su aprobación en 2016, la comisaria Viviane Reding presentó esta reforma como el reglamento que definía el marco normativo de la protección de datos para las próximas décadas. Posteriormente, cuando el reglamento estaba casi aprobado, en el año 2016, Viktor Mayer-Schönberger, uno de los principales expertos europeos en protección de datos y *big data*, describió el nuevo marco normativo como «un paso intermedio que apunta hacia la necesidad de hacer evolucionar la protección de datos más allá del viejo paradigma, aunque todavía no está plenamente comprometido con ello» (Mayer-Schönberger y Padova, 2016, págs. 331-332). Es discutible cuál de las dos opiniones define mejor el alcance de la primera reforma de la protección de datos en la Unión Europea.

El resultado final de esta reforma aparece aún incompleto y deberá esperarse a su aplicación y a cómo será recibida por las autoridades de control[1] e implementada por los legisladores nacionales. En este sentido, el tema del *big data* puede constituir el campo de pruebas donde valorar si la solución propuesta por el legislador europeo responde efectivamente a los retos que plantea la evolución de la tecnología.

(1)Véase el art. 51 y sigs., Reglamento (UE) 2016/679.

Anticipándonos al análisis que se contiene en este módulo, puede ya afirmarse que el Reglamento (UE) 2016/679 (RGPD en adelante) no parece ser capaz de superar la «prueba» del *big data*. Esto no quiere decir que dicho reglamento no proporcione soluciones útiles para la resolución de los problemas planteados por el nuevo paradigma de gestión de la información, pero es solo un punto de partida. Parece que el legislador europeo carece de la perspectiva necesaria, teniendo en cuenta los efectos de las aplicaciones tecnológicas que determinarán el horizonte de los próximos veinte años.

En este sentido, el reglamento no supone una innovación radical de las características que, a partir de la década de los 90, definieron el marco regulador de la Unión Europea. Sin embargo, desde una perspectiva social y tecnológica, la última década del siglo pasado fue un tiempo completamente diferente del actual. Baste decir que en el año en que se aprobó la Directiva 95/46, los usuarios de internet eran una porcentaje limitado de la población, Google y Facebook no existían y el procesador del ordenador más potente del mundo (la «ASCI red») no superó la barrera de 1 teraflop de capacidad de cálculo.

Este enfoque «conservador» del legislador europeo plantea tres límites a una regulación eficaz del *big data*: la interpretación conservadora del principio de finalidad del tratamiento, la incertidumbre de la autodeterminación del individuo en el presente contexto y la dimensión individual del uso de los datos que debería extenderse a una visión más colectiva del uso de los mismos.

1. El *big data* y los principios de protección de datos personales

En Europa, a lo largo de los últimos cuarenta años, se ha adoptado un modelo de regulación del tratamiento de los datos personales basado en unas características distintivas. En particular, a partir de las primeras «generaciones» de leyes sobre protección de datos, se afirmó la centralidad del principio de limitación de la finalidad del tratamiento. Este principio se entiende como la fijación de un propósito específico que permite la gestión de datos desde el momento de su recogida[2].

(2)Véase el art. 5.1 (b), Reglamento (UE) 2016/679; Article 29 Data Protection Working Party (2013).

Otro principio fundamental, relacionado con el anterior, es el principio de minimización de los datos, que supone limitar la recogida y el tratamiento de los datos a aquellos estrictamente necesarios en relación con las finalidades del tratamiento[3]. Posteriormente, a lo largo de los años 80, el efecto de la revolución tecnológica, provocada por la difusión de los ordenadores personales junto al advenimiento del marketing directo, comportó reconocer un papel prominente al consentimiento de los interesados[4].

(3)Véase el art. 5.1 (c), Reglamento (UE) 2016/679.

(4)Véanse los arts. 6.1 (a) y 7, Reglamento (UE) 2016/679; Article 29 Data Protection Working Party (2011).

Por una parte, la difusion de los ordenadores hizo accesible a muchos tanto su utilización como el conocimiento relativo a su funcionamiento (aspectos antes restringidos a un número muy limitado de expertos). Efectivamente, los mainframes de los 70 fueron, de hecho, grandes ordenadores accesibles solamente a expertos calificados. La gente común no tenía ningún tipo de conocimiento y solamente percibió el riesgo potencial de un tratamiento masivo de datos que podía efectuarse a través de este tipo de máquinas. Por esta razón, en aquellos años, los legisladores intentaron proporcionar una respuesta a esta preocupación por medio de las primeras leyes de protección de datos (véase Losano, 1981, pág. 472), a través del reconocimiento de los derechos relativos al acceso a los datos y el establecimiento de autoridades reguladoras independientes.

Esta primera generación de normas carece de toda referencia al consentimiento de los interesados, que constituye una herramienta para lograr la autodeterminación de la persona. Sin embargo, el sujeto tenía poca importancia en un contexto caracterizado por la falta de conciencia de las modalidades de tratamiento. Hay que añadir que, a causa de la magnitud de la inversión requerida, en muchos casos estas primeras bases de datos fueron creadas por la administración pública. En consecuencia, el carácter público de los objetivos perseguidos excluyó cualquier cuestión relacionada con el consentimiento de los ciudadanos.

Por estas razones, con el advenimiento del ordenador personal, el tratamiento de datos personales comprende a la gran masa de la población. Hay que añadir que, durante los años 80, los datos personales fueron cada vez más utilizados por el sector privado con fines comerciales y para definir los perfiles individuales de los consumidores de manera más detallada (creación de perfiles). En consecuencia, ya no se trataba simplemente de recoger la información para finalidades puramente organizativas (por ejemplo, listado de los clientes y provededores), sino que los datos empiezan a adquirir un valor económico y competitivo específico.

Si se combina el conocimiento del tratamiento de la información con el valor económico de la misma, ello hace razonable que las personas reclamen tener un papel más significativo en la circulación de datos que les conciernen. De ahí el reconocimiento, incluso por parte de los legisladores, del consentimiento como condición para el tratamiento de los datos personales.

La protección de los datos personales se coloca en el contexto más amplio de los derechos de la personalidad y la explotación comercial de estos atributos no comporta una mutación de su esencia. Los datos siguen estando estrechamente relacionados con la persona y no se produce posteriormente una cosificación de la misma. Esto implica la imposibilidad de aplicar una lógica puramente propietaria a la información personal y seguir modelos extranjeros que son muy favorables a la asimilación de la información personal al campo de la propiedad intelectual (véase Schwartz, 2004, pág. 2055 y sigs.; Samuelson, 2000, pág. 1125 y sigs.; Lessig, 1999. Para una visión diferente, véase Cohen, 2000, pág. 1373 y sigs.; Rodotà, 1995, pág. 55).

Si los datos personales circulan, ello ocurre principalmente en virtud del consentimiento del afectado. Sin embargo, ello se produce dentro de un marco teórico que se caracteriza por una cierta complejidad, debido a la presunta falta de disponibilidad de los derechos de la personalidad (Mantelero, 2007, pág. 69 y sigs.; Alpa y Resta, 2006, pág. 594 y sigs.). En cualquier caso, la circulación de estos datos es de forma «controlada» (Rodotà, 1991, pág. 522; Orestano, 2003, pág. 147 y sigs.; Giannantonio, 1999, pág. 484 y sigs.; Zeno-Zencovich, 1995, pág. 438) en la medida que el titular del derecho (el interesado) conserva toda una serie de prerrogativas respecto de «sus informaciones» (las informaciones que le conciernen) y el derecho a revocar en cualquier momento el consentimiento otorgado (Resta, 2000, pág. 310 y sigs.; Cafaggi, 1998, pág. 619 y sigs.).

El consentimiento del afectado tendría una naturaleza dual, similar a la que tiene en otros casos de derechos de la personalidad susceptibles de explotación económica. El consentimiento del interesado es, por un lado, un acto unilateral que consiste en una autorización del uso del atributo de la personalidad que alguien hace. De esta manera, se excluye la ilegitimidad del uso (Messinetti, 1998, pág. 350 y sigs.; Resta, 2000, pág. 306 y sigs.; Sica, 2001, pág. 629 y sigs.; Navarretta, 1999, pág. 338), lo que permite la negociación de esos atributos y, más específicamente, de los datos personales. Por otro lado, el consentimien-

to es la expresión de la soberanía del individuo respecto de la información personal que le concierne, que es necesario para la comunicacion de datos a terceros, en ausencia de limitaciones específicas fijadas por la ley.

En este sentido, si bien es cierto que el consentimiento es solo una de las causas de legitimación del tratamiento de datos y que todas ellas tienen la misma importancia[5], sin embargo está claro que solo el consentimiento es el instrumento con el que se ejerce de un modo pleno la autodeterminación informativa del interesado respecto de los datos que le conciernen (Orestano, 2003, pág. 176; Rodotà, pág. 79 y sigs.). En todos los otros casos, esta autodeterminación informativa –en donde no se excluye[6]– se limita a su dimensión negativa, dentro de los límites reconocidos por la ley[7].

(5)Véase Article 29 Data Protection Working Party (2011).

(6)Véase el art. 6.1.c) y d), Reglamento (UE) 2016/679.

(7)Véase el art. 21, Reglamento (UE) 2016/679.

Este fue el modelo de regulación que se definió a finales de los años 80 y que cristalizó en la Directiva 95/46/CE (Gambaro, 1985, pág. 524 y sigs.; Alpa y Bessone, 1984; Alpa, 1981, pág. 29 y sigs.; Alpa, 1979, pág. 65 y sigs.; Rodotà, 1973). Este modelo se basaba en el presupuesto según el cual las personas son capaces de conocer los métodos y los fines del tratamiento, de entenderlos en términos de sus posibles consecuencias y de elegir libremente si proporcionar o no sus datos para los fines indicados.

Además, el consentimiento puede ser considerado como tal solo si es libre e informado (tal y como ha sido estudiado en módulos correspondientes a otras asignaturas). Estos requisitos del consentimiento, sobre los que se basa la noción de autodeterminación, están perdiendo fuerza frente a la utilización de técnicas de tratamiento de la información basada en el *big data*.

Antes de examinar estos puntos críticos, es necesario aclarar de forma preliminar que el concepto de *big data* que se utiliza para evaluar cómo esta tecnología afecta el derecho a la protección de datos no coincide plenamente con la noción más en uso, que se deriva de la cultura informática.

Aunque hay, de hecho, muchas definiciones de *big data*, la mayoría de ellas se centran en la capacidad técnica para recoger y procesar grandes cantidades de información de acuerdo con el paradigma de las tres V (volumen, velocidad y variedad). Las nuevas formas de tratamiento se caracterizan por procesar datos en gran cantidad (volumen), por una gran capacidad de crecimiento (velocidad) y por una variedad de tipos de formatos (variedad).

Sin embargo, estas variables descriptivas no son muy útiles para evaluar el impacto social del *big data*, lo que representa el punto central de la reflexión jurídica en materia de protección de datos llevada a cabo por la doctrina, los tribunales y el legislador. De hecho, con referencia a la protección de la persona respecto al tratamiento de la información, las principales cuestiones no se refieren al volumen, la velocidad, y la variedad de los datos, sino al hecho que estos datos pueden ser procesados por medio de software que tiene la capaci-

dad de obtener un nuevo conocimiento predictivo acerca de la evolución de los fenómenos a que se refieren los datos. Este conocimiento puede entonces ser empleado para tomar decisiones que involucren a individuos y grupos (V. Bollier, 2010; Mantelero, 2017, pág. 139 y sigs.).

Desde esta perspectiva, a los efectos de este módulo, es más apropiado referirse a la noción de *big data analytics*, que es el software de análisis predictivo al que se ha hecho referencia, en lugar de hablar de *big data*. Ello es así, precisamente, teniendo en cuenta la creciente importancia del aspecto inherente a la nueva generación de información más que la dimensión relativa a los aspectos cuantitativos y cualitativos de los datos.

En particular, la llegada del *big data analytics* (en adelante también simplemente *analytics*) sugirió la adopción de un nuevo paradigma en el campo de los estudios sociales. En este terreno, el tradicional enfoque estadístico y basado en encuestas se completa o se sustituye mediante el análisis centrado en el *big data*. Este nuevo paradigma se caracteriza por el importante papel desempeñado por la visualización de datos, lo que hace posible el análisis de los flujos de información en tiempo real con el fin de identificar sus trayectorias de propagación y predicción de tendencias futuras. Además, el uso de algoritmos de análisis permite sacar correlaciones desconocidas entre grandes cantidades de datos, sobre la base de que se desarrollan modelos predictivos (Mayer-Schönberger y Cukier, 2013, pág. 59 y sigs.).

Este enfoque, que se basa en las tendencias y en las supuestas correlaciones entre los datos, implica un modo diferente de diseño de la investigación social en el que no hay ninguna hipótesis específica de búsqueda predeterminada. Son los mismos datos y su dinámica los que sugieren las posibles relaciones entre hechos y comportamientos. De esta manera, el análisis de los datos y la dinámica de estos son los elementos que sugieren cuáles serán los aspectos específicos que merecen ser sometidos a una investigación que luego se puede llevar a cabo utilizando herramientas estadísticas tradicionales.

> Así, por ejemplo, en los últimos tiempos, las palabras utilizadas para realizar consultas mediante los motores de búsqueda (Bing) han sido utilizadas para predecir la aparición de tumores del páncreas (Paparrizos, White y Horvitz, 2016, pág. 737 y sigs.).

Teniendo en cuenta el enfoque brevemente descrito, se deduce que en el momento de la recolección de datos solo pueden formularse hipótesis de investigación muy generales, ya que las inferencias potenciales deducibles de los datos son aún desconocidas. Por consiguiente, la finalidad específica del tratamiento[8] solo puede ser identificada en un momento posterior, cuando la aparición de algunas inferencias ponga de relieve la utilidad de la información específica con el fin de detectar ciertos aspectos, que ulteriormente podrán ser verificados y analizados.

[8] Véanse los arts. 5.1 (b) y 6.1 (a), Reglamento (EU) 2016/679.

En relación con el Reglamento (UE) 2016/679, es posible observar cómo se pueden utilizar los datos para fines distintos del fin original, si no son incompatibles con este primer fin[9]. Esta posibilidad proporcionada por las normas del reglamento podría ser utilizada para justificar la redefinición de los fines que, como se ha dicho, es propia de la utilización de la informaciión en el contexto del *big data*[10]. Estas reglas asumen que hay un fin inicial y específico. Sin embargo, con frecuencia la recopilación de información en el contexto del *big data* se lleva a cabo a gran escala con fines muy genéricos o persigue finalidades específicas que son muy distintas de aquellas para las que los datos fueron recogidos en un principio.

(9)Véanse los arts. 5.1 (b) y 6.4, Reglamento (EU) 2016/679.

(10)Véase Mayer-Schönberger y Padova (2016, pág. 326 y sigs.).

Por último, existen diferentes formas de tratamiento y análisis de datos, tales como algoritmos de machine learning, capaces de generar su propio conocimiento como resultado de una fase de «formación». Durante dicha fase, un conjunto de datos predefinidos se utiliza para corregir los errores del algoritmo, orientando así este mismo a que lleve a cabo asociaciones correctas. En este caso, a diferencia de los anteriores, se identifican desde el principio las finalidades de los sistemas de análisis. Sin embargo, la manera en que se procesan los datos y el resultado final del proceso de data mining permanecen en gran medida desconocidos, siendo estos algoritmos similares a «cajas negras» cuya dinámica interna es parcialmente impredecible.

En general, tanto el *big data analytics* orientado a identificar tendencias y correlaciones, como los algoritmos de *machine learning*, que se pretende que sean críticos, surgen en el modelo tradicional de protección de datos personales, que está enfocado en la autodeterminación individual con referencia a las informaciones relativas al sujeto. De hecho, hay casos en los que los fines y las modalidades del tratamiento se conocen solo parcialmente y falta o uno u otro de los elementos básicos que permiten a la persona evaluar las consecuencias de sus decisiones.

Se debe añadir que, en el contexto del *big data*, la complejidad del procesamiento agrava aún más los límites ya conocidos a la autodeterminación real de la persona con respecto al tratamiento de los datos que cuestionan el modelo de consentimiento informado en general. Por lo tanto, en lo que se refiere a la información que deberá facilitarse cuando los datos se obtengan del interesado (art. 13 RGPD), la complejidad de los procesos y (en el caso del *big data*) la dificultad de definir adecuadamente los posibles usos de los datos llevan a los responsables a proporcionar una información sobre los fines del tratamiento que, en algunas ocasiones, es genérica y vaga o bien extremadamente analítica y técnica.

En ambos casos, sin embargo, las personas a las que se refieren los datos no están interesadas en conocer la información relativa a las modalidades del tratamiento. Si por el contrario se preocupan por ello, encontrarán información que no es suficientemente clara. Por ejemplo, se hallan frases como esta: «los

datos serán utilizados para mejorar su experiencia de usuario». O bien se ofrece una explicación ampliamente detallada que describe los aspectos técnicos y legales. De ahí la creciente falta de atención al contenido de la información que se facilita cuando se recogen los datos, que aún es mayor en el contexto del *big data*, donde la complejidad de los procesos y la falta de definición de la finalidad específica del tratamiento hace aún menos relevante el papel de la información facilitada a los interesados.

Además, este escenario se agrava por la presencia de los cambios económicos, sociales y tecnológicos que caracterizan a menudo muchos de los servicios de la sociedad de la información. Estos últimos años han sido testigos de una creciente concentración de las actividades de tratamiento de datos muy intensivas, tanto por el tamaño global de algunos grandes operadores del sector (por ejemplo, Google), como a causa de los fenómenos de fusión o adquisición que han afectado a las empresas que tienen gran cantidad de información. El número limitado de entidades que operan en diferentes sectores donde se lleva a cabo una amplia recolección de datos (por ejemplo, en el sector del crédito), la falta de normas uniformes y el «efecto red» comportan que, en la práctica, quede limitada la libertad de elección de los usuarios de los servicios.

De todas estas observaciones se deduce que el consentimiento es cada vez menos una herramienta útil para alcanzar la autodeterminación de las personas respecto a «sus» datos. De hecho, paradójicamente, el consentimiento puede convertirse en la solución más fácil para recopilar datos para los fines más diversos, teniendo en cuenta los límites que afectan tanto las informaciones facilitadas a los interesados como el consentimiento, entendido como expresión de verdadera libertad de elección del individuo.

Existen también dificultades para aplicar el principio de minimización en el entorno del *big data* porque, en virtud de este principio, los datos recogidos deben ser «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados»[11]. Más aún, la mencionada incertidumbre sobre las finalidades del tratamiento y la propensión a una mayor recogida posible de datos, que frecuentemente caracteriza las estrategias que utiliza el *big data*, determinan una difícil aplicación automática de este principio en este contexto.

(11)Véase el art. 5.1.c, Reg. (EU) 2016/679.

Lo mismo puede afirmarse en relación con algunas categorías y notas distintivas que tradicionalmente caracterizan la disciplina de protección de datos. En particular, ante el potencial de las nuevas tecnologías analíticas, parece ponerse en cuestión la noción misma de datos personales en referencia tanto a la distinción entre los datos personales y los datos anónimos (considerando 26 del Reglamento), como a la división interna entre datos comunes y sensibles (art. 9 RGPD).

En este sentido, varios estudios han demostrado que las informaciones contenidas en un conjunto de datos anónimos se pueden re-identificar parcialmente en algunos casos sin recurrir a soluciones técnicas costosas (Narayanan, Huey y Felten, 2016, pág. 357 y sigs.; Narayanan y Felten, 2014; de Montjoye, Radaelli, Kumar Singh y Pentland, 2015, pág. 536 y sigs.; Ohm, 2010, pág. 1701 y sigs.; United States General Accounting Office, 2011, pág. 68 y sigs.; Golle, 2006, pág. 77 y sigs.; Sweeney, 2000; Sweeney, 2000). Esto plantea la posibilidad de considerar superada la tradicional dicotomía entre los datos personales y los anónimos. En consecuencia, se plantea adoptar una perpectiva diferente en la que los datos personales y los anónimos son polos extremos de una escala progresiva que se caracterizaría por un nivel creciente de anónimización.

En la evaluación de este nivel, el enfoque debería ser, por lo tanto, sobre la fuerza de las soluciones técnicas adoptadas con el fin de impedir que los datos se pudieran re-identificar. Por consiguiente, debería adoptarse una noción relativa de datos anónimos basada en el riesgo de re-identificación, el cual sería directamente proporcional al esfuerzo que se necesitara para volver a re-identificar la información en términos de tiempo, recursos y costes (considerando 26 del Reglamento).

Por último, con respecto a los datos sensibles, mientras en el pasado fue indudable la diferente naturaleza que connota esta subcategoría de datos y la dicotomía existente entre los datos comunes y los sensibles, actualmente el uso del *big data analytics* hace que sea posible extraer información sensible a partir de datos no sensibles, hecho que no permite establecer una clasificación previa en abstracto. A modo de ejemplo, considérese en este caso las informaciones acerca de la movilidad, que comúnmente se reputan como no sensibles. Sin embargo, si esta información se analiza a gran escala, permite extraer patrones de movilidad relativos a personas identificables a partir de los cuales es posible inferir, por ejemplo, la asistencia a lugares de culto, la participación en iniciativas políticas o el estado de salud (observando, por ejemplo, la presencia regular en las immediaciones de hospitales especializados en el tratamiento de enfermedades específicas) (Mantelero, 2015, pág. 309 y sigs.).

1.1. El *big data* en el marco del Reglamento General de Protección de Datos

A pesar de los conflictos que existen entre algunos de los principios fundamentales de la reglamentación europea de la protección de datos y la naturaleza del *big data*, en el nuevo reglamento hay varias disposiciones que pueden utilizarse para hacer frente a los retos que plantea este nuevo paradigma y aplicarlos en este contexto para que sea posible el uso de los *analytics*.

En este sentido, el art. 5.1.b RGPD admite que los datos recogidos pueden tratarse ulteriormente para fines distintos de los iniciales, siempre que no sean incompatibles con dichos fines. Para evaluar si existe esta compatibilidad entre los fines, el considerando 50 y el art. 6.4 establecen que se tenga en cuenta lo siguiente:

«**a)** cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento[12];

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.»

[12]Véase el considernado 50, Reg. (EU) 2016/679.

Estas normas sobre el cambio de finalidad se pueden aplicar al *big data* cuando los *analytics* se utilicen para fnalidades que no sean muy distintas de las iniciales y, por esta razón, pueden tener solo una aplicación limitada en el entorno del *big data*. En este terreno, los resultados potenciales en términos de inferencia de correlaciones entre los datos y el comportamiento son en gran parte impredecibles. Sin embargo, esto no excluye que en algunas aplicaciones específicas del *big data*, con un enfoque muy específico, pueda ser posible una aplicación potencial de estas normas, sobre todo a la luz de la referencia a nociones generales, tales como «las expectativas razonables del interesado»[13] y «las posibles consecuencias para los interesados del tratamiento ulterior previsto.»

[13]Véase el considernado 50, Reg. (EU) 2016/679.

Más específicamente, la referencia a «las posibles consecuencias para los interesados del tratamiento ulterior previsto» es importante en términos de la evaluación de la compatibilidad entre los riesgos del uso de los datos, que parece desplazar la evaluación de la compatibilidad entre las finalidades del tratamiento. Lamentablemente, este cambio de perspectiva, desde el enfoque de las finalidades a la atención de los riesgos, sigue quedando marginado en el reglamento, a pesar de que podría ser la manera más adecuada para hacer frente a los retos del big data analytics[14].

[14]Véase el siguiente parágrafo número 6.

Finalmente, de acuerdo con el art. 13.3 del reglamento, «cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.» Esta también parece una obligación difícil de cumplir en el caso del *big data*, a causa del gran número de interesados.

Otra forma para legitimar el tratamiento de datos para fines diferentes cuando se utiliza el *analytics* puede ser invocar el art. 5.1.b del reglamento, que permite el tratamiento ulterior de los datos con fines estadísticos. Respecto a esta opción, según observan Mayer-Schönberger y Padova (2016), la excepción estadística (véanse también los arts. 14.5.b, 17.3.d, 21.6, 89, 89.2 y el considerando 162) solo se puede aplicar a una gama limitada de casos. En este sentido, el Parlamento Europeo señaló que el «el tratamiento de datos personales con fines estadísticos solo puede dar como resultado datos agregados que no se pueden aplicar de nuevo a los individuos». Pero este no es el caso de muchas aplicaciones relativas al *big data*, donde los resultados del análisis predictivo de grupos se aplican a individuos específicos que forman parte de la multitud de cada grupo, al igual que sucede en el caso de la aplicación de los *analytics* respecto a la creación de perfiles individuales.

Por último, se deben tener en cuenta las disposiciones del art. 22 del reglamento sobre las decisiones individuales automatizadas. En este sentido, la primera observación se refiere al ámbito de aplicación de este artículo, es decir, solo un número limitado de casos en los que se utiliza el *big data* consisten en procesos para la toma de decisiones automatizadas. En muchos casos, los *analytics* son herramientas de soporte para decisiones que serán tomadas por personas. Y ello a pesar de que el papel de la persona que toma la decisión sea secundario, en la medida en que los resultados de los algoritmos gozan del atractivo de la objetividad matemática. Asimismo, la complejidad de la gestión de los datos y la posición subordinada a los mismos de aquellos que tienen que adoptar decisiones en sus organizaciones comportan que sea difícil asumir el riesgo potencial de una decisión diferente de la sugerida por el algoritmo.

Además, cuando existe un proceso automatizado para tomar decisiones, el reglamento no proporciona indicaciones específicas acerca de los valores que deben inspirar este proceso o la adopción de métodos participativos para definir el diseño de los *analytics*. Solo se reconoce a los interesados «el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión», a excepción de los casos en los que las decisiones automatizadas están autorizadas por la ley, que proporciona «medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de los interesados». Se reconoce en esta disposición un derecho general «a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar», pero esta disposición puede ser fácilmente derogada en base a finalidades contractuales o del consentimiento del interesado (art. 22.2.a y c, RGDP) y, dados los límites conocidos del consentimiento del interesado en términos de autodeterminación, esto reduce el nivel de la protección efectiva proporcionada por esta norma.

2. El análisis de los riesgos en materia de protección de datos y el *big data* (arts. 35.1 y 37.7 RGPD)

A pesar de la decisión del legislador de la Unión Europea de mantener el paradigma tradicional, fijado en 1995, el Reglamento (UE) 2016/679 introduce disposiciones específicas que, aunque no se centran específicamente en el *big data*, producen un efecto en este contexto y contribuyen a mejorar el nivel de protección de los interesados.

En este sentido, el cambio progresivo del enfoque normativo de la autodeterminación individual a las formas de responsabilidad basadas en la evaluación de los riesgos[15] (por ejemplo, la evaluación de impacto relativo a la protección de datos, la consulta previa de las autoridades de protección de datos, la adopción de estándares) reduce parcialmente las dificultades en la regulación del *big data* que resultan del enfoque tradicional de la protección de datos. En este sentido, los preceptos del Reglamento (UE) 2016/679 sobre la gestión del riesgo en el tratamiento de datos representan una importante evolución hacia un enfoque basado en el riesgo y ofrecen una solución parcial a los posibles efectos negativos de la utilización del *big data analytics*.

(15)Véase Article 29 Data protection Working Party (2017); CNIL (2015a, 2015b, 2012); Article 29 Data Protection Working Party (2014, 2013, 2011); Trilateral Research & Consulting (2013); Vedder and Naudts (2017); Böröcz, (2016, págs. 467-480).

Sin embargo, la principal limitación de estas normas es la relación existente entre la evaluación del riesgo y los fines del tratamiento de datos, porque los límites que caracterizan la aplicación del principio de finalidad en el contexto del *big data* afectan necesariamente a la evaluación de riesgos.

De hecho, cualquier evaluación se relaciona con el uso de datos para un propósito específico y, de acuerdo con el Reglamento (UE) 2016/679, la finalidad del procesamiento de datos debe ser «específica, explícita y legítima», y ha de estar definida en el momento de la recogida de datos. Sin embargo, esto no es coherente con el uso transformador de datos por parte de organismos privados y públicos que se lleva a cabo a través del *big data analytics*.

Otro límite se refiere a la naturaleza de la evaluación del riesgo que se requiere en el reglamento. En este sentido, la noción de riesgo adoptada por el legislador europeo se centra en los «daños y perjuicios materiales o inmateriales» que perjudican a los «derechos y libertades de las personas físicas»[16]. Esto está en línea con una gestión del riesgo que presupone un enfoque basado en la protección de los derechos y no en una evaluación indistinta entre riesgos y beneficios (Wright y Raab, 2014, pág. 277 y sigs.).

(16)Considerando 75, Reg. (EU) 2016/679.

De acuerdo con esta perspectiva, cuando existe un riesgo de perjuicio que no puede ser mitigado o excluido, el tratamiento de datos se convierte en ilegal, a pesar de la presencia de cualquier razón legítima, como el consentimiento del interesado. En este sentido, el considerando 75 del reglamento establece una larga lista de casos en los que el tratamiento de datos es ilegal.

Cabe señalar que este considerando no limita estas hipótesis a la seguridad del tratamiento de datos, sino que también tiene en cuenta el riesgo de discriminación y «cualquier otro perjuicio económico o social significativo». Esta noción de impacto del riesgo, de la que se hace eco el art. 35 del reglamento, representa un paso importante en la dirección de una evaluación del impacto de la informática que ya no se centra principalmente en la seguridad de los datos[17], sino en una evaluación más robusta y más amplia de los diferentes aspectos que pueden ser afectados por el uso de los datos[18].

(17)Véase el art. 32. Reg. (EU) 2016/679.

(18)Véase también el art. 29 Data protection Working Party (2014, pág. 15).

Esta atención a las consecuencias económicas y sociales del uso de datos asume una relevancia significativa en el contexto del *big data*, donde los *analytics* forman parte de los procesos de toma de decisiones y pueden tener impactos negativos en las personas, en términos de discriminación[19] más que de seguridad de los datos[20]. Sin embargo, las disposiciones del reglamento no ofrecen un marco regulador adecuado para una evaluación de este tipo de resultado negativo.

(19)Véase The White House, Executive Office of the President (2016); European Data Protection Supervisor (2015).

(20)Véase European Parliament (2017).

El enfoque de la mitigación de riesgos adoptado por el reglamento aún parece lejos de la idea de una evaluación del impacto sobre la privacidad que tenga también en cuenta la dimensión ética y social (Privacy, Social and Ethical Impact Assessment – PESIA). Véase el proyecto H2020 «VIRT-EU: Values and ethics in Innovation for Responsible Technology in Europe» <http://www.virteuproject.eu/>, que consiste en una evaluación múltiple y participativa de los riesgos, donde las potenciales consecuencias negativas del tratamiento no solo se miden en cuanto a la protección de la información, sino que también incluyen las consecuencias sociales del uso de los datos y sus impactos en la aplicación de los valores éticos[21].

(21)Véase la sección 3.3.

Con respecto a la evaluación de los aspectos éticos en el contexto de la investigación e innovación, véase Shelley-Egan *et al.*:

«La evaluación del impacto ético de la investigación y la innovación considera tradicionalmente los potenciales daños sociales, los riesgos y las implicaciones que tienen para los derechos fundamentales, la justicia, el bienestar de los ciudadanos y el bien común. Dichas evaluaciones pueden requerir que se tengan en cuenta los impactos potenciales en la salud, el medio ambiente, el trabajo, el ocio, las relaciones sociales, la política, los valores y en otros aspectos. Para lograr todo ello, con frecuencia la evaluación del impacto ético combina el análisis ético con el análisis del impacto social, con futuros estudios, con el análisis del escenario y con la evaluación de la tecnología. El compromiso con las partes interesadas y el diálogo público son otras acciones incluidas en la evaluación del impacto ético, puesto que las primeras pueden ayudar a anticipar los usos e impactos y pueden manifestar sus preocupaciones e intereses como parte del proceso de evaluación ética.»

Shelley-Egan *et al.*, 2014, pág. 42 y sigs.

La falta de esta perspectiva más amplia representa un límite, ya que el uso del *big data analytics* en los procesos de toma de decisiones plantea importantes cuestiones sobre los valores que deben impulsar la futura sociedad basada en el algoritmo. Por otra parte, con referencia a la dimensión colectiva, los legisladores deben también reflexionar sobre el papel que los diferentes actores sociales pueden desempeñar en la evaluación de los impactos sociales del uso de datos[22] (Mantelero, 2016, pág. 249 y sigs.).

[22] Véase la sección 3.4

3. Reconsiderar el papel del consentimiento y el principio de limitación de la finalidad desde una perspectiva de la centralidad del riesgo

Como se ha afirmado en los apartados anteriores, el Reglamento (UE) 2016/679, aunque introduzca cambios significativos en la existente disciplina europea del tratamiento de datos, no cuestiona las bases del modelo actual. En particular, la importancia del consentimiento informado[23] y la especificidad de la finalidad del tratamiento, tal como se define en el momento inicial de la recolección de datos, que siguen siendo elementos fundamentales de la nueva regulación. En este sentido, el legislador de la Unión Europea parece no haber advertido la tensión extrema que caracteriza la aplicación del principio de finalidad en el contexto del *big data* ni los problemas que afectan a la autodeterminación de la persona.

[23] Véanse los arts. 6.1.a, 7, 8, y 9.2.a Reglamento (UE) 2016/679.

Sin embargo, teniendo en cuenta las consideraciones expresadas en los puntos anteriores, no parece que este enfoque sea satisfactorio para asegurar la protección efectiva de los individuos frente a la creciente importancia de los algoritmos en nuestra sociedad. Por esta razón, es necesario abrir un debate sobre este tema e identificar nuevas propuestas *de iure condendo* para superar los límites de las normas existentes.

En este sentido, la doctrina ya ha intentado encontrar alternativas que, a veces, han planteado una revisión radical del marco legal existente. Así, por ejemplo, se ha propuesto reemplazar el principio de finalidad por un amplio concepto de interés legítimo. Ello dejaría en manos de los sujetos privados, que son quienes tratan los datos, la evaluación y el equilibrio entre los diferentes intereses, según una interpretación que, sin duda alguna, favorecería los intereses de las empresas (Moerel, 2014).

Véase Moerel-Prins:

> «the principle of purpose limitation will have to be abandoned as a separate criterion. The time has come to recognize the legitimate interest principle as the principal (and only) test for all the various phases of the life cycle of personal data» and «this approach would result in a regulatory framework within which data collection and processing is permissible, unless it is deemed to be "unfair" or "not legitimate" and therefore unlawful.»
>
> Moerel-Prins, 2016, pág. 43 y sigs. y 75 y sigs.

Una perspectiva diferente y más garantista, que se sugiere en este módulo y será desarrollada más ampliamente en las páginas siguientes, acepta expresamente la idea de que los datos se recogen para propósitos múltiples y cambiantes (Tene-Polonetsky, 2012, pág. 64), que se pueden definir solo de mane-

ra genérica cuando empieza el tratamiento (Mantelero, 2014, pág. 84 y sigs.; Gonçalves, 2017, donde la autora sugiere una interesante comparación con la evaluación de impacto ambiental).

Este modelo se centra en los varios usos específicos de la información que cada vez se hace respecto de los datos recogidos, como consecuencia de las inferencias sugeridas por los *analytics*. En este sentido, se sugiere hacer una evaluación previa de los posibles riesgos asociados a cada uso bajo la supervisión de autoridades de protección de datos.

Desde esta perspectiva, la evaluación del riesgo se convierte en el medio para definir mejor los fines específicos de cada uso de los datos y reducir los posibles efectos negativos del tratamiento. Esto también debería inducir al legislador a reconsiderar y reducir el papel atribuido al consentimiento respecto al tratamiento de datos a favor de un modelo centrado en el riesgo y a reforzar el papel de las autoridades de supervisión con respecto a la evaluación preliminar del impacto potencial de los diferentes usos de los datos.

Un modelo similar ha sido también sugerido, recientemente, por otros autores que están de acuerdo en destacar la oportunidad de mirar a los fines de los usos específicos de la información en lugar de los fines generales de la recogida de los datos. Sin embargo, esta doctrina, a diferencia de la posición que se acaba de describir, no otorga un papel destacado a las autoridades de control, al tiempo que sugiere la transición desde el «ritual» del consentimiento a unos «procedimientos de evaluación deliberada *ex ante* no solo de los beneficios, sino también de los riesgos y daños potenciales para los individuos asociados a un uso determinado de los datos, así como la necesidad de idear e implantar estrategias concretas de mitigación». En este sentido, el Reglamento (UE) 2016/679, se considera más como un punto de partida que como el desembarco de un nuevo paradigma (Mayer-Schönberger-Padova, 2016, págs. 326 y 332; Cate-Mayer Schönberger, 2013).

En particular, el modelo propuesto aquí se centra en los diferentes usos específicos de la información recogida que se lleven a cabo cada vez. Si este modelo fuera adoptado por el legislador, ello podría conducir a definir un marco de regulación más eficiente y coherente con el uso efectivo de los datos.

Este modelo podría también combinarse con una aplicación más amplia de la noción de interése legítimo[24] como base jurídica para el tratamiento (Moerel, 2014). De esta manera, las entidades privadas podrían obtener más fácilmente los datos de los interesados y también volver a utilizarlos para diferentes propósitos, pero solo sobre la base de un análisis de los riesgos relacionados con cada uso específico de los datos, sin perjuicio del derecho de los interesados a ejercer su «opt-out» respecto de los datos tratados.

(24)Véase el art. 6.1.f, Reglamento (UE) 2016/679.

La solución *de iure condendo* aquí propuesta (para un análisis más amplio, véase Mantelero, 2014) y ahora brevemente descrita difiere de la adoptada por el reglamento, principalmente porque considera que la evaluación de impacto se requiere para todos los tratamientos, mientras que en el reglamento se requiere solo para casos particulares[25]. En las hipótesis en las que se requiere la evaluación de impacto, en virtud del art. 35.3.a del reglamento, se pueden incluir diferentes casos de uso del *big data*. Sin embargo, hay situaciones en las que el uso de los *analytics* no conduce necesariamente a una «evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas», porque la evaluación puede no tener el carácter sistemático y extensivo de las solicitudes, no ser totalmente automatizada, o no producir «efectos jurídicos».

(25)Véanse los arts. 35.1 y 35.3, Reglamento (EU) 2016/679.

Debido al carácter predictivo del *big data* y la incapacidad para definir de manera previa los efectos específicos del tratamiento, parece más apropiado hacer una evaluación de impacto en todos los casos en que se utilizan estos métodos de análisis para tratar información personal. Por último, cabe señalar cómo el Reglamento, en la definición de los casos en los que el análisis de riesgo debe llevarse a cabo mediante las formas de evaluación de impacto, de forma explícita hace referencia a la finalidad del tratamiento mediante la adopción de un criterio que se ve afectado por la criticidad que ya se ha mencionado, debido a las dificultades de conciliar lo que deberían ser los fines «determinados, explícitos y legítimos» especificados en el momento de la recogida de los datos y las operaciones de análisis que efectivamente se realizan por medio de los *analytics*.

La evaluación del impacto respecto a la protección de datos en el marco del reglamento[26] se caracteriza entonces como una autoevaluación, sujeta únicamente en algunos casos a ser examinada por las autoridades de protección de datos[27], y cuyos resultados no son públicos. La solución aquí propuesta, sin embargo, sugiere la recuperación del modelo basado en la autorización que caracterizó las primeras regulaciones relativas al tratamiento de datos, que necesita el examen previo de la autoridad de supervisión (Bygrave, 2014, pág. 183 y sigs.) y, además, la publicidad de los resultados de la evaluación de los riesgos.

(26)Véase el art. 35, Reglamento (UE) 2016/679.

(27)Véase el art. 36, Reglamento (UE) 2016/679.

En cuanto al papel que debe reconocerse a la autodeterminación del individuo, existe una analogía entre la situación de los años 70 y la presente caracterizada por el uso de los *analytics*. Ambos contextos se caracterizan por la incapacidad de las personas ordinarias de entender la manera de tratar los datos y cómo esta puede afectar a cada sujeto, lo que es consecuencia de un avance significativo, tanto en calidad como en cantidad, de los procesos de gestión de datos.

Por lo tanto, en ambos casos, se manifiesta la utilidad limitada de la noción de autodeterminación informativa entendida como una autoevaluación que los individuos sean capaces de realizar y se está haciendo cada vez más claro el beneficio de un modelo de regulación que pretende garantizar un uso seguro de la información, entendido como la ausencia de consecuencias negativas o, al menos, la mitigación de estos riesgos. Esta es una solución similar a aquella que se ha adoptado en la regulación de la seguridad de los productos (véase, por ejemplo, el proceso de autorización a la comercialización de los productos farmacéuticos), donde no se le pide al usuario que verifique la naturaleza y las funciones de los productos para que evalúe los riesgos, sino que en cambio se ofrecen bienes cuya seguridad ya ha sido objeto de control.

Del mismo modo, en presencia de complejos sistemas de tratamiento de datos o de archivos de datos afectados por efectos de lock-in tecnológico y social, la evaluación de los riesgos y beneficios debería pesar siempre menos en los individuos, a través del mecanismo de consentimiento informado, y en su lugar debería adoptarse un sistema transparente y general de análisis de los riesgos que fuera capaz de garantizar una gestión de datos sin causar perjuicios al individuo ni a la sociedad. En este sentido, la decisión del legislador europeo de poner el enfoque del reglamento en las normas que se refieren al análisis de riesgos representa, sin duda, un paso adelante en esta dirección, a pesar de que va más allá de las limitaciones mencionadas anteriormente.

Sin embargo, en el reglamento el análisis de riesgos parece limitarse a aquellos que se examinan típicamente en relación con los datos personales y que se refieren, principalmente, a la seguridad y lealtad del tratamiento. Esto no tiene en cuenta un análisis más amplio que incluya el impacto social relacionado con el uso del análisis predictivo para tomar decisiones y que sería más adecuado para hacer frente a los problemas que plantea el *big data*.

4. El *big data* y los límites de la dimensión individual

En el escenario de grandes volúmenes de datos, el análisis de la información se ve cada vez menos interesado en el individuo y en su identidad y, por el contrario, más a menudo se centra en el estudio a gran escala de grupos de personas, a veces muy amplios, hasta incluir millones. Esto ocurre porque, cada vez más, la finalidad de la recogida y el análisis de datos es estudiar el comportamiento de estos grupos y predecir su evolución futura en lugar de elaborar perfiles individuales, por lo que los individuos se tienen en cuenta como pertenecientes a un grupo o a otro (véanse, por ejemplo, las técnicas de discriminación de precios) (Executive Office of the President of the United States, Council of Economic Advisers, 2015; Rosenblat-Randhava-Boyd-Peña Gangadharan-Yu, 2014; Federal Trade Commission, 2014; Dixon-Gellman, 2014, págs. 21 y 44).

En este sentido, tanto en el sector comercial como en el contexto de la administración pública (por ejemplo, en relación a las políticas sociales o a la prevención de la delincuencia) (Perry-McInnis-Price-Smith-Hollywood, 2013; Rieke-Robinson-Yu, 2014; Mantelero-Vaciago, 2014, pág. 175 y sigs.; Ferguson, 2012, pág. 259 y sigs.; van Brakel-De Hert, 2011, pág. 163 y sigs.), se tiende a definir las estrategias generales a gran escala en base a las representaciones de la sociedad proporcionadas por algoritmos predictivos (Pasquale, 2015; Mayer-Schönberger y Cukier, 2013; Bollier, 2010; Rubinstein, 2013, pág. 74 y sigs.). Estas estrategias se aplican después a personas identificadas en virtud de su pertenencia a uno o más grupos formados por los analytics (Federal Trade Commission, 2014; Hildebrandt, 2006, pág. 548 y sigs.).

Este enfoque sobre las categorías creadas por las herramientas de análisis predictivo conduce a los responsables a adoptar soluciones comunes para todas las personas que estén clasificadas en la misma categoría. Por esta razón, el uso de los datos va más allá de la dimensión individual y adquiere una dimensión colectiva (Mantelero, 2016, pág. 238 y sigs.; Vedder, 1999, pág. 275 y sigs.; Rodotà, 1997, pág. 134 y sigs.), en particular con referencia a las posibles consecuencias perjudiciales para todos los individuos afectados (Peña Gangadharan, Eubanks y Barocas, 2014; Crawford, Faleiros, Luers, Meier, Perlich y Thorp, 2013).

La relevancia de esta dimensión colectiva no es nueva en el contexto de la regulación del tratamiento de datos y, de hecho, esta normativa se originó con la elaboración de normas ante los temores de posibles clasificaciones y de discriminación de grupos de personas. Sin embargo, la protección de datos se basa en el modelo del derecho subjetivo, mientras que la dimensión colectiva emergente de protección con respecto al tratamiento en el contexto del *big data* no se limita necesariamente a hechos o datos que se relacionan directa-

mente con una persona específica, sino que también incluye grupos de individuos no reconducibles a la tradicional noción sociológica de grupo. Se trata, de hecho, de grupos que no están predeterminados, tales como las minorías o los grupos políticos, sino que son creados por los algoritmos y pueden ser reconfigurados de forma continua por el algoritmo. En un contexto de esta naturaleza, fluido y variable, no se puede conocer a priori si una persona será clasificada como perteneciente a un grupo particular.

En términos legales, la atención a la dimensión colectiva no se puede resolver sumariamente recurriendo a una simple representación a gran escala de los derechos individuales y de las cuestiones relacionadas con el procesamiento de datos, ya que la diferente perspectiva adoptada puede implicar la aparición de nuevos ámbitos de protección. En este sentido, la dimensión colectiva de protección de datos se refiere a distintos intereses, que no son necesariamente la simple suma de intereses individuales (Newman, 2004, pág. 127 y sigs.).

En concreto, esta dimensión colectiva se centra principalmente en el uso de la información (Cate y Mayer-Schönberger, 2013a; Cate y Mayer-Schönberger, 2013b, pág. 67 y sigs.; Mantelero, 2014, pág. 643 y sigs.), en lugar del secreto (Bloustein, 1978, pág. 182) y la calidad de los datos. En este contexto, los posibles riesgos ya no solo se refieren a los habituales asociados con el tratamiento de datos (como el uso ilegal de datos personales o la falta de seguridad en la gestión de la información), sino a aquellos relativos a la potencial discriminación relacionada con la clasificación predictiva de los comportamientos de grupo y, en consecuencia, de los sujetos que los integran (The White House, Executive Office of the President, 2014; Zarsky, 2013, pág. 1510 y sigs.; Vedder, 1997, pág. 215 y sigs.).

En este sentido, cabe destacar que aquí no se está haciendo referencia tanto a prácticas desleales que se caracterizan por fines discriminatorios intencionales, en general, prohibidos y sancionados (European Commission, 2013; Ellis y Watson, 2015; Schreurs, Hildebrandt, Kindt y Vanfleteren, 2010, pág. 258 y sigs.), sino más bien a casos de discriminación no intencionada derivada de errores en el diseño, la implementación y el uso de modelos analíticos basados en el *big data* (Citron y Pasquale, 2014, pág. 1 y sigs.; Burnbaum, 2013). Estos errores darán lugar a representaciones distorsionadas de la sociedad que pueden comprometer de manera significativa los interesados afectados por las decisiones tomadas a partir de los resultados ofrecidos por los algoritmos (Sweeney, 2013, pág. 44 y sigs.; Bosker, 2013; Crawford, 2013; Lerman, 2013, pág. 55 y sigs.; Rieke, Robinson y Yu, 2014). Así, por ejemplo, los consumidores que están clasificados como «con dificultades financieras» pertenecen a un grupo de entidades formadas por personas que «en los principales años de trabajo de sus vidas […] incluyendo a muchos padres solteros, luchan con algunas de las rentas más bajas y una escasa acumulación de riqueza» y ese grupo de perfil está asociado a la siguiente predicción: «no especialmente leales a ninguna institución financiera, se sienten incómodos al pedir prestado dinero y creen que están mucho mejor teniendo hoy lo que quieren, puesto que nunca saben

lo que les deparará el mañana» (Federal Trade Commission, 2014, pág. 20). De esto se desprende la consecuencia negativa evidente de errores de clasificación que pueden afectar tanto al individuo como a todo el grupo y que están asociados a especificas evaluaciones de predicción.

Por último hay que señalar que, en varios casos, el potencial de estas discriminaciones puede que no se base tanto en los perfiles individuales como en las informaciones comunes a aquellos que pertenecen a una determinada categoría, sin identificación directa de los interesados. Por esta razón, las disposiciones de las leyes existentes contra la discriminación no pueden ser eficaces en la prevención de las consecuencias negativas de estas prácticas si se toman sobre una base colectiva. De ello se deriva un elemento más a favor de una consideración específica de la dimensión colectiva de la utilización de información sobre grupos de individuos.

5. La dimensión ética y social del impacto del uso del *big data*

Centrando la atención en el uso colectivo de los datos, las implicaciones son significativas y no se limitan a los mencionados riesgos relativos a la discriminación, sino que también plantean cuestiones más generales sobre la consistencia del uso de algoritmos respecto a los valores éticos y sociales de una comunidad. En este sentido, la cuestión no se refiere solamente a los perjuicios potenciales en relación con el resultado proporcionado por el algoritmo (por ejemplo, decisiones de tipo discriminatorio), sino a la decisión misma de transformar la sociedad en una representación mediatizada por modelos matemáticos, así como la identificación de los valores introducidos en tales modelos para tomar decisiones por parte de quien crea los algoritmos.

Teniendo en cuenta los aspectos que se refieren a los valores que inspiran los modelos lógicos de los algoritmos, hay que señalar cómo la dimensión que hay que valorar no es estática y puede variar de un contexto cultural a otro, como es el caso incluso respecto de la noción de privacidad en tanto que valor social (A. F. Westin, 1970, pág. 183 y sigs.; Whitman, 2004, pág. 1151 y sigs.; Bygrave, 2002, pág. 327; Nissenbaum, 2010, pág. 231). De ahí la dificultad de identificar un conjunto común de principios éticos y sociales que puedan considerarse ampliamente compartidos y que se tomen como referencia para evaluar las posibles consecuencias de las aplicaciones basadas sobre el *big data*.

Precisamente por las razones que se acaban de mencionar, parte de la doctrina ha puesto de relieve la dificultad de definir directrices éticas vinculantes que sirvan como una dirección en el uso del *big data*. Sin embargo, la misma doctrina ha identificado un posible marco común de referencia en los valores reconocidos y confirmados por las cartas internacionales de derechos fundamentales, que también pueden servir como un indicador de la relación entre los diversos valores (Wright, 2011, pág. 199 y sigs.).

Sin embargo, la referencia a las cartas fundamentales de los derechos solo puede proporcionar una indicación abstracta, especialmente en relación con el equilibrio entre los distintos intereses que tienen que ser protegidos. Por lo tanto, será necesario proceder a una ponderación respecto al caso concreto, teniendo en cuenta la naturaleza específica y el contexto de la concreta aplicación de los *analytics*. Este equilibrio de intereses en el caso particular tiene necesariamente que basarse en una evaluación de los posibles efectos negativos de la utilización de los datos que, en presencia de recogida y tratamiento de datos complejos, no se puede dejar solamente a los interesados ni a la auto-evaluación del responsable del tratamiento de los datos, sino que debe

implicar la participación activa de todas las partes implicadas. De ahí la importancia de las posibles formas de representación de los intereses colectivos que puedan entrar potencialmente en juego.

En este sentido, puede servir de referencia la gestión de dichos intereses en el derecho laboral, como formas ya conocidas de representación de los intereses colectivos y aplicado al tratamiento de datos. Junto con los instrumentos que proporciona el derecho laboral, existen herramientas de reconocimiento, protección y gestión de los intereses colectivos en sectores como la protección del consumidor y la protección del medio ambiente.

Todas estas situaciones se caracterizan por el desequilibrio de poder que afecta a una de las partes directamente involucradas. Además, en muchos casos, los intereses contrapuestos se refieren a ámbitos en los que el uso de las nuevas tecnologías hace que sea difícil que los usuarios sean conscientes de las posibles consecuencias negativas que comportan. De ahí las limitaciones de una protección que se configure solo en términos individuales, afectada por el desequilibrio característico de algunas relaciones de poder y la falta de conocimiento e información. Dichas barreras pueden ser superadas más fácilmente a nivel colectivo.

La misma situación de desequilibrio existe respecto de las aplicaciones del *big data*, ya que, como se ha señalado, las personas a menudo no saben, o al menos no serían capaces de entender, las modalidades que caracterizan esta forma de tratamiento de datos. Ello comporta que no puedan negociar el tratamiento de la información que les concierne, teniendo un conocimiento adecuado de los posibles riesgos, individuales y colectivos, que ello pueda implicar. En este sentido, como en los casos mencionados anteriormente, la articulación de alguna forma de representación de los grupos de personas potencialmente afectadas por el tratamiento podría reducir este desequilibrio y mejorar también la toma de conciencia y comprensión del proceso de tratamiento.

No obstante, cabe señalar que la diferente naturaleza de los grupos en cuestión tendría un impacto en términos de representación. Así, por ejemplo, en el caso del tratamiento de información de los trabajadores, los empleados representan un grupo previamente establecido en el que los miembros son conscientes de la identidad de grupo y conocen tanto a los otros miembros como las relaciones con su contraparte empresarial. De modo diferente, aquellos cuyos datos son objeto de la agregación mediante algoritmos no son conscientes de pertenecer a un grupo concreto en lugar de otro ni de la identidad de las otras personas objeto de la misma clasificación.

A esto se añade que los grupos en cuestión no son estáticos, sino que pueden estar sujetos a modificaciones continuas debidas al diferente peso asignado a cada una de las variables, lo que comporta el movimiento de las personas de

un grupo a otro. Por último, los interesados no conocen los atributos comunes que caracterizan a todos aquellos que están clasificados en el mismo grupo, porque solo los responsables del tratamiento conocen esa información.

A partir de esta «estructura de geometría variable» de los grupos creados por medio de los algoritmos y de estas limitaciones en términos de conocimiento, se deduce que las partes interesadas tienen una percepción muy limitada de las implicaciones potenciales que pueden afectarlas de forma colectiva. Si bien estas limitaciones expuestas, por un lado, pueden constituir un obstáculo para una representación de los intereses colectivos organizados, por el otro ponen de relieve la necesidad de dicha representación. Esta, sin embargo, no puede pasar a través de un procedimiento electivo como en el ámbito del derecho laboral, puesto que falta el conocimiento mutuo de las partes interesadas.

Ante los inconvenientes que puede comportar la aplicación de la representación colectiva propia del derecho laboral, puede resultar útil acudir a las normas relativas a la protección del consumidor. Efectivamente, existen similitudes entre la situación del consumidor y del afectado por el *big data*. En el caso del consumidor, existen intereses colectivos (tales como la seguridad del producto o la competencia desleal), a pesar de que las personas potencialmente afectadas no tengan relación entre sí. En estos casos, los remedios individuales se pueden combinar con otros remedios de carácter colectivo. Estos pueden consistir en la posibilidad de recurrir a las acciones colectivas, reconociendo el papel de representación de los intereses colectivos a las asociaciones que los protegen, así como recurriendo a autoridades independientes que deban salvaguardar activamente dichos intereses.

Algunas de estas soluciones se pueden utilizar en el contexto del *big data*, si bien algunas de ellas tendrán una eficacia más limitada en este contexto. Este es el caso, por ejemplo, de las acciones colectivas, que parecen ser menos eficaces a causa de la dificultad de reaccionar de una manera oportuna respecto a los posibles tratamientos que muchas veces pueden llevarse a cabo con el desconocimiento de los afectados (por ejemplo, Parlamento Europeo, 2013; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, 2013a, 2013b). Más decisivo, en cambio, podría ser el papel de las asociaciones que representan los intereses de grupos o categorías de personas que utilizan los servicios basados en el *big data*.

En referencia a este último aspecto, el art. 80 del Reglamento (UE) 2016/679 representa un primer reconocimiento del papel potencial de estas asociaciones aunque, en el actual estado preliminar de la aplicación del reglamento, esta norma parece solo parcialmente satisfactoria. En particular, el artículo reconoce el derecho del individuo a dar un mandato a una asociación, cuya finalidad es la protección de los derechos de las personas afectadas, «para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado

en el artículo 82». Esto implica que siempre se necesita la iniciativa de un individuo y, por lo tanto, alguien debería tener la conciencia y la capacidad de entender los efectos del uso del *big data*. Pero, como se ha dicho antes, los algoritmos son muchas veces «cajas negras» para los interesados. Más eficaz podría ser la posible aplicación del segundo párrafo del art. 80, donde se reconoce que cualquier entidad, organización o asociación sin ánimo de lucro tiene derecho a presentar una reclamación ante la autoridad de control. Sin embargo, la aplicación de esta disposición se deja a la discreción de los Estados miembros.

Hay que añadir que, como se mencionó anteriormente, los intereses que se revelan acerca del uso de la información en el contexto del *big data* trascienden los tradicionales intereses relacionados con la protección de datos y afectan un escenario más amplio que se centra en el impacto social del uso de los datos. En este sentido, por ejemplo, uno de los puntos más críticos puestos de relieve (entre otros, Barocas y Selbst, 2016, pág. 671 y sigs.; Schreurs, Hildebrandt, Kindt y Vanfleteren, 2010; Peña Gangadharan, Eubanks y Barocas, 2014) se refiere a los riesgos potenciales de discriminación que pueden afectar a algunos grupos. Por este motivo, es necesario preguntarse cuáles deben ser los organismos que han de garantizar la protección de las personas respecto a estos posibles riesgos.

En particular, en los distintos sistemas legales, la competencia relativa a la lucha contra la discriminación está fragmentada entre diferentes organismos independientes y, generalmente, no se atribuye a las autoridades responsables de protección de datos[28]. Esto implica encontrarse ante autoridades que adoptan enfoques diferentes, disponen de herramientas diversas para contrastar los comportamientos ilícitos y no necesariamente cooperan en la solución de los casos que presentan repercusiones diferenciadas en términos de impacto.

(28)Véase Comisión Europea (2013).

En este escenario, hay que señalar que el elemento central en la evaluación de los riesgos asociados al análisis de grandes volúmenes de datos se refiere a la capacidad de analizar y evaluar las modalidades de tratamiento de los datos, en tanto que el tratamiento de la información es el factor común en todas estas situaciones, independientemente de la naturaleza del daño potencial a los diferentes intereses colectivos. Por esta razón, las autoridades de protección de datos podrían desempeñar un papel clave en el proceso de evaluación de los riesgos, precisamente debido a su experiencia en el campo del tratamiento de datos, a pesar de que no se centran en las implicaciones sociales específicas del tratamiento.

Por otro lado, si en su lugar se adoptara un enfoque diferente, se deberían tener en cuenta las diversidades de los posibles efectos negativos derivados de la utilización del *big data* (la discriminación, las prácticas de consumo desleal, el control social, etc.), y deberían estar implicadas diversas autoridades competentes. Sin embargo, en este caso, el resultado final podría ser una toma de decisiones fragmentadas y potencialmente conflictivas respecto de la resolu-

ción de los diversos casos. Asimismo, las evaluaciones –en ausencia de conocimientos específicos– podrían dar lugar a una subestimación de los aspectos relativos a la utilización de datos, que constituyen el núcleo común de todas las aplicaciones centradas en el *big data*.

Hay que añadir que las autoridades de protección de datos ya tienen una larga experiencia en hacer frente a cuestiones relacionadas con el impacto en la sociedad mediante la utilización de la información. En la mayoría de los casos, estas autoridades han demostrado la capacidad para llevar a cabo evaluaciones exhaustivas de los riesgos potenciales de las nuevas aplicaciones tecnológicas, que no se limitan a la persona, sino que también tienen en cuenta la dimensión colectiva de la utilización de los datos. En consecuencia, dichas autoridades han demostrando que son también capaces de sugerir medidas adecuadas para reducir los riesgos aquí examinados[29]. Además, para proteger los intereses relacionados con los datos personales, tales autoridades están acostumbradas a llevar a cabo una ponderación entre los intereses individuales y colectivos de naturaleza diferente. Ello demuestra su capacidad para desempeñar el papel más importante, en términos de intereses protegidos.

(29)Véase, por ejemplo, Article 29 Data Protection Working Party (2014).

Por último, en relación con el objeto y los métodos que deben caracterizar el análisis de riesgos, en línea con las observaciones anteriores, la evaluación debe centrarse no solo en la seguridad de los datos y en el tratamiento correcto de los mismos (por ejemplo, el respecto de los fines, el respeto del procedimiento, la legitimidad del acceso a la información), sino que también debe tener en cuenta las implicaciones éticas y sociales relacionadas con el uso colectivo del *big data* en cada proyecto donde se adopte esta tecnología. Consecuentemente, la evaluación no debería ser auto-referencial y realizada exclusivamente por los responsables del tratamiento de los datos, sino que debería contemplar tanto la participación de las categorías de las personas que pueden resultar interesadas, como llevarse a cabo bajo la supervisión de las autoridades de protección de datos.

Dada la complejidad de las evaluaciones relacionadas con el uso del *big data* que afecta a aspectos diferentes, en el análisis de los riesgos potenciales deben tomar parte no solo los expertos legales en materia de protección de datos, sino también auditores externos con experiencia específica y multidisciplinar en los campos de la ética y las ciencias sociales. Esta misma fase de evaluación constituirá una oportunidad para identificar mejor los grupos de personas potencialmente afectadas por los riesgos asociados al tratamiento, por lo que también sería una fase preliminar para garantizar la participación efectiva de todos los afectados. De esta manera, se podrían superar parcialmente las dificultades antes mencionadas de representación efectiva de los intereses colectivos relacionados con el uso de los datos, especialmente cuando las autoridades de control en el campo de la protección de datos, y en la supervisión del proceso, promovieran esa participación.

De esta manera, se aplicaría un nuevo modelo de análisis de los riesgos relacionados con el uso de la información en el contexto del *big data*, un modelo más abierto tanto en lo que respecta a los intereses tomados en cuenta como con referencia a la participación de los diversos grupos de interés. Sin embargo, el Reglamento (UE) 2016/679, que pretende tener en cuenta los efectos discriminatorios y los perjuicios «social[es] significativo[s][30]» y que adopta una estrategia nueva y más robusta de análisis de riesgos, no parece percibir plenamente la complejidad y versatilidad de las implicaciones del uso de los *analytics*. Del mismo modo, también parece poco capaz de mirar más allá de un modelo centrado en la autodeterminación individual y de abrirse a la consideración de la dimensión colectiva, de manera que aun así solo ofrece soluciones iniciales que carecen de un adecuado desarrollado operacional[31].

(30)Véase el considerando 75, Reglamento (UE) 2016/679.

(31)Véase el art. 80, Reglamento (UE) 2016/679.

Desde el Consejo de Europa parecen venir respuestas más satisfactorias y que se centran específicamente en los aspectos críticos relacionados con el uso del *big data*. Especialmente, de las directrices sobre el tratamiento de datos personales y del *big data*[32]. Estas últimas, que se discutirán brevemente en el siguiente apartado, esbozan un proceso de evaluación de los riesgos que tiene en cuenta el impacto ético y social de la aplicación de los *analytics* y también sugieren un enfoque más participativo con referencia al análisis de riesgos, que se ve como una herramienta para superar las limitaciones que afectan al consentimiento de los interesados.

(32)Véase Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Estrasburgo, 23 de enero de 2017 <https://rm.coe.int/CoERMPublicCommonSearch Services/DisplayDCTM Content?documentId=09000016806ebe7a>.

6. Las directrices para la protección de los datos personales en el uso del *big data*. Las indicaciones del Consejo de Europa

A pesar de que las directrices establecidas por el Consejo de Europa sobre la base del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal no tienen el mismo impacto que el Reglamento (UE) 2016/679 en términos de eficacia y de aplicación directa, representan sin embargo un texto interesante que, en varios puntos, esboza una nueva forma de encarar las cuestiones relativas a la utilización del *big data analytics*.

Antes de examinar brevemente las disposiciones de las «Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data» (en adelante, las directrices), se debe mencionar la naturaleza y las características específicas de este instrumento y del entorno en que se inserta. En particular, en el contexto del Convenio 108 sobre la protección de las personas respecto al tratamiento de los datos personales, las directrices son instrucciones prácticas y operacionales proporcionadas por el Consejo de Europa a los Estados Miembros. En este caso, los destinatarios de las directrices son principalmente los responsables y los encargados del tratamiento, con la intención de facilitar la aplicación de los principios de la Convención en la específica área del *big data*.

Con especial referencia a las directrices que aquí se tratan, hay que señalar que, a diferencia de otras adoptadas anteriormente por el Consejo de Europa[33], relativas a situaciones o cuestiones concretas, en este caso el enfoque se centra en el uso de una tecnología específica (*big data*), independientemente de la aplicación de la misma en un campo específico. Esto implica, necesariamente, que las directrices proporcionan reglas de carácter general y no se pueden tener en cuenta las características específicas, en términos de restricciones legales que caracterizan el uso de datos en diferentes áreas.

(33)Véase Guidelines for prison and probation services regarding radicalisation and violent extremism (2016); Guidelines of the Committee of Ministers of the Council of Europe on child friendly justice (2010).

La toma de conciencia de las cuestiones críticas que plantean las nuevas formas de procesamiento de datos basados en el *big data analytics* caracteriza a todo el sistema de las directrices y, en este contexto, los principios del Convenio 108 se interpretan con el fin de proporcionar soluciones adecuadas, que también tienen en cuenta el «especifico contexto social y tecnológico» así como la «falta de conocimiento por parte de los individuos» respecto a las aplicaciones en cuestión[34].

(34)Véase Guidelines, Section I (Introduction).

Desde esta perspectiva, el derecho a «controlar sus datos personales y el tratamiento de estos datos» reconocido por el Convenio 108 del Consejo de Europa, en su versión «modernizada» pendiente de aprobación[35], se contextualiza con respecto a la realidad del *big data*, en el que los procesos de recogida y análisis de datos se caracterizan por su complejidad y la falta de transparencia. Con este fin, las directrices no tienen en cuenta el concepto de control como limitado solamente a un control individual (ya que es el modelo centrado en el consentimiento informado), sino que adoptan una noción más amplia de control sobre el uso de la información personal, en la que «el control individual evoluciona en una evaluación más compleja del impacto múltiple de los riesgos relacionados con el uso de los datos»[36].

(35)Véase Draft Modernised Convention 108 («Teniendo en cuenta que es necesario garantizar la dignidad humana y la protección de los derechos humanos y las libertades fundamentales de cada individuo y […] la autonomía personal basada en el derecho de la persona a controlar sus datos personales y el tratamiento de esos datos.») <https://www.coe.int/en/web/data-protection/modernisation-convention108>.

(36)V. Guidelines, Section I (Introduction).

Esto lleva a ir más allá de la dimensión individual de la protección de datos y a tener en cuenta la dimensión colectiva del tratamiento de datos, también contemplando el posible riesgo en términos de conflicto con los valores éticos y sociales, como se ha mencionado anteriormente. En este sentido, la primera sección de la parte cuarta («Principios y directrices») insta tanto a los titulares como a los encargados a «tomar en consideración el posible impacto del tratamiento del *big data* propuesto y sus implicaciones éticas y sociales más amplias».

Aunque las directrices reconocen la dificultad de definir los valores que deben ser tenidos en cuenta en la evaluación social y ética de la utilización de los datos, no renuncian a identificar un modelo capaz de satisfacer esa necesidad. De este modo, en particular, se define una estructura de tres niveles, que van desde los principios fundamentales y generales a los valores éticos y sociales que deben tenerse en cuenta en relación con la aplicación específica que haga uso del *big data*.

Los valores esenciales son identificados como los reconocidos por los textos internacionales de los derechos humanos y las libertades fundamentales, empezando por la Convención Europea de Derechos Humanos[37] (Wright, 2011, pág. 201 y sigs.). Estos textos proporcionan una especie de cartografía en relación con los derechos que es compartida por todos los Estados miembros del Consejo de Europa y que no solo establece derechos y valores de suma importancia, sino también las relaciones entre éstos.

(37)Véase Guidelines, Section IV, § 1.2.

En la medida en que la evaluación del impacto en términos éticos y sociales es, por su naturaleza, dependiente del contexto social, las cartas internacionales pueden proporcionar solo pautas muy generales. Por ello las directrices tienen también en cuenta los «valores éticos comúnmente aceptados en la comunidad o comunidades relevantes y no deberían perjudicar los intereses sociales, los valores y las normas». Por esta razón, se requiere que el uso de datos se lleve a cabo teniendo en cuenta esta dimensión local y respetando los valores que le son propios[38].

(38)Véase Guidelines, Section IV, § 1.2.

Por último, para evaluar los intereses importantes en lo que respecta a cada aplicación específica del *big data*, el último nivel está destinado a ser una adaptación al caso concreto de las directrices generales que derivan de las fuentes ahora mencionadas. En este sentido, las directrices sugieren la adopción de «comités de ética ad hoc» que ya se utilizan en algunos casos en el campo del análisis de los datos. Estos comités deben identificar los valores éticos específicos que deben salvaguardarse respecto a un uso concreto de datos, proporcionando directrices más detalladas y centradas en los aspectos específicos del contexto particular, tanto en términos de equilibrio de intereses como de evaluación de los riesgos.

En términos generales, las directrices colocan el proceso de evaluación de riesgos en un contexto más amplio que un enfoque preventivo[39] (Costa, 2012, pág. 14 y sigs.; Gonçalves, 2017, pág. 20; Pieters, 2011, pág. 455, «generalizado a la tecnología de la información, puede servir como impulsor para que el gobierno considere, por fin, las implicaciones sociales del desarrollo de las TI. Mientras que el principio preventivo tradicional apunta a la sostenibilidad medioambiental, la prevención en la información se dirigiría a la sostenibilidad social»; Raab y Wright, 2012, pág. 364; Lynskey, 2015, pág. 83), que debe caracterizar a cada nueva aplicación tecnológica que pueda implicar riesgos potenciales para el individuo y la sociedad. Desde esta perspectiva, también se requiere que los responsables del tratamiento adopten políticas preventivas para hacer frente y mitigar de manera adecuada los riesgos potenciales relacionados con el uso del big data analytics[40].

(39)Véase Guidelines, Section IV, § 2.1 («Dada la creciente complejidad del tratamiento de datos y el uso transformativo del *big data*, las partes deberán adoptar un enfoque preventivo en la regulación de la protección de datos en este ámbito»).

(40)Véase Guidelines, Section IV, § 2.2.

Específicamente, el proceso de análisis de riesgos, en línea con la teoría general en esta materia, se divide en cuatro fases diferentes: 1) la identificación de los riesgos; 2) el análisis del impacto potencial de los riesgos identificados; 3) la adopción de soluciones destinadas a excluir o reducir los efectos de estos riesgos; 4) la vigilancia continua o periódica de la eficacia de las soluciones adoptadas.

En relación al tratamiento de datos personales, y respecto a este modelo tradicional de análisis y gestión de riesgos, el aspecto innovador es la amplia gama de intereses considerados en el proceso de evaluación, que va más allá del concepto tradicional de protección de datos y que tiene en cuenta, específicamente, el derecho a la no discriminación y los impactos negativos que el uso del *big data* puede tener sobre los valores éticos y sociales.

En relación al análisis del modo de efectuar el análisis de los riesgos, dada la complejidad de esta evaluación y la diversidad de los aspectos a tener en cuenta, las directrices sugieren que la misma sea llevada a cabo «por personas con el conocimiento y las calificaciones profesionales apropiados para evaluar los diferentes impactos, incluidas las dimensiones legales, sociales, éticas y técnicas[41]». Además, la dimensión colectiva de los posibles efectos de la utilización

(41)V. Guidelines, Section IV, § 2.6.

(42)V. Guidelines, Section IV, § 2.7.

de los datos lleva a destacar la importancia de la participación activa en la evaluación de los riesgos y de los diferentes grupos de personas que pueden resultar de alguna manera afectados por cada uso específico de los datos[42].

Dada la complejidad de esta evaluación y la continua evolución tanto de los riesgos potenciales como de las medidas para hacerles frente, se reconoce finalmente que las autoridades de protección de datos podrían desempeñar un papel importante. Dicho rol consistiría en dar soporte a los responsables del tratamiento, proporcionándoles conocimientos técnicos sobre el estado de arte de los procesos de tratamiento y las medidas de seguridad, así como por medio de la elaboración de directrices más detalladas relativas al proceso de evaluación de riesgos que se recomienda en las Guidelines[43].

(43)V. Guidelines, Section IV, § 2.8.

En cuanto a los interesados, el análisis de los riesgos y de los posibles impactos de la utilización de los datos puede dar lugar a una mejor comprensión de los fines del tratamiento. Por esta razón, el conocimiento de los resultados de este análisis debe formar parte del deber de transparencia que ha de caracterizar todo tratamiento de datos. El cumplimiento de esta obligación de información, de hecho, podría incrementar la sensibilización de las personas ante las elecciones que están llamadas a realizar relativas al uso de la información que les afecta. Por supuesto, la publicidad de la evaluación de impacto, de acuerdo con la sugerencia de la doctrina (Richards y King, 2013, pág. 43; Mantelero, 2013, pág. 234; Wright 2011, pág. 222), debe llevarse a cabo «sin perjuicio del secreto garantizado por la ley». Por lo tanto, donde haya una necesidad de secreto, ello comportará que el responsable del tratamiento proporcione «cualquier información confidencial en un anexo separado del informe de evaluación». En este caso, aunque el anexo no sea público, las autoridades de protección de datos personales pueden tener acceso al mismo en el ejercicio de sus funciones y en el curso de sus investigaciones[44].

(44)V. Guidelines, Section IV, § 3.3.

Además de proporcionar pautas sobre el análisis y la gestión de riesgos que forman el núcleo central de las directrices, en estas existen disposiciones adicionales que es preciso destacar por su enfoque innovador. Así, por ejemplo, en relación con el consentimiento informado, se sugiere que la información proporcionada a los interesados, además de contener los resultados de la evaluación de los riesgos mencionados anteriormente, se facilite «por medio de una interfaz que simule los efectos del uso de datos y su impacto potencial en el interesado, en un enfoque de aprendizaje desde la experiencia[45]». También hay que señalar que, de acuerdo con estas directrices, el consentimiento no se puede considerar libre cuando haya un «claro desequilibrio de poder entre el interesado y el responsable que afecte las decisiones del primero en relación con el tratamiento[46]».

(45)V. Guidelines, Section IV, § 5.1.

(46)V. Guidelines, Section IV, § 5.3.

Finalmente, en las Guidelines hay una sección especifica sobre el papel de la intervención humana en la toma de decisiones basadas en el *big data analytics*, en que se confirma que el recurso a estas soluciones debe preservar «the

(47)V. Guidelines, Section IV, § 7.1.

autonomy of human intervention in the decision-making process[47]». En este sentido, se enfatiza que aquellos que deben tomar decisiones deberían ser libres de no constreñirse necesariamente al resultado de las sugerencias proporcionadas por el *big data analytics* si existen «argumentos razonables» que justifiquen una decisión diferente[48]. En aquellos casos en los que la decisión pueda afectar significativamente los derechos individuales o producir efectos jurídicos, las directrices aclaran que aquellos que deben tomar las decisiones, si el interesado lo pide, proporcionen «las razones subyacentes del tratamiento, incluidas las consecuencias para el interesado de dichas razones[49]».

(48)V. Guidelines, Section IV, § 7.4.

(49)V. Guidelines, Section IV, § 7.3.

Resumen

La realidad del *big data* constituye el campo de pruebas donde valorar si la solución propuesta por el legislador europeo responde efectivamente a los retos que plantea la evolución de la tecnología. En este módulo, se ha demostrado cómo las normas del RGPD no parecen ser capaces de proporcionar soluciones útiles para la resolución de los problemas planteados por el nuevo paradigma de gestión de la información, sino que son solo un punto de partida.

El marco regulador de la Unión Europea, a partir de las primeras leyes sobre protección de datos, se basa en el presupuesto según el cual las personas son capaces de conocer los métodos y los fines del tratamiento y de entenderlos en términos de posibles consecuencias. Sin embargo, en el contexto del *big data*, la complejidad del tratamiento agrava los límites ya conocidos a la autodeterminación real de la persona. De igual modo, también existen dificultades en la aplicación de los principios de minimización y de finalidad del tratamiento.

Aunque en el nuevo reglamento hay varias disposiciones que pueden utilizarse para hacer frente a los retos que plantea el nuevo paradigma del *big data*, especialmente con referencia a la evaluación de los riesgos en materia de protección de datos, muchas veces se trata de disposiciones que, en el entorno del *big data*, pueden tener solo una aplicación o un efecto limitado.

Por esta razón, la doctrina ha proporcionado soluciones alternativas. El Consejo de Europa ha intentado ir más allá de la dimensión individual de la protección de datos y tener en cuenta la dimensión colectiva del tratamiento de datos. Asimismo, también se contempla el posible riesgo en términos de conflicto con los valores éticos y sociales.

Aunque el Reglamento (UE) 2016/679 no parezca percibir plenamente la complejidad y versatilidad de las implicaciones del uso de los *analytics*, la necesidad de asegurar la protección efectiva de los individuos frente a la creciente importancia de los algoritmos hace evidente la importancia del debate y del estudio crítico de este tema.

Bibliografía

(2011). «Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent». <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.

(2011). «Article 29 Data Protection Working Party. Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications». <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf>. Acceso: 27 de febrero de 2017.

(2013). «Article 29 Data Protection Working Party. Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart GridTask Force». <http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-ecommendation/files/2013/wp209_en.pdf>. Acceso: 27 de febrero de 2017.

(2014). «Article 29 Data Protection Working Party. Working Document on surveillance of electronic communications for intelligence and national security purposes».

(2014). «Article 29 Data protection Working Party. Statement on the role of a risk-based approach in data protection legal frameworks». <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>. Acceso: 27 de febrero de 2017.

(2017). «Article 29 Data protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679». <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137>. Acceso: 13 de abril de 2017.

Alpa, G.; Bessone, M. (a cura di), (1984). *Banche dati, telematica e diritti della persona*. Padova: Cedam.

Alpa, G. (1979). «Privacy e statuto dell'informazione». *Riv. dir. civ.* (I, pág. 65 y sig.).

Alpa, G. (1981). «Raccolta di informazioni, protezione dei dati e controllo degli elaboratori elettronici». *Foro it.* (V, pág. 29 y sig.).

Alpa, G.; Resta, G. (2006). *Le Persone e la Famiglia. 1. Le persone fisiche e i diritti della personalità*. Torino: UTET.

Alpa. G.; Zeno-Zencovich, V. (eds.) (1985). *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*. Napoli: Jovene.

Bosker, B. (2013). «Google's Online Ad Results Guilty Of Racial Profiling, According To New Study». *The Huffington Post* (2 de mayo de 2013) <http://www.huffingtonpost.com/2013/02/05/online-racial-profiling_n_2622556.html>.

Barocas, S.; Selbst, A. D. (2016). «Big Data's Disparate Impact». *Cal. L. Rev* (104, pág. 671 y sig.).

Koops, Bert-Jaap (2015). «The trouble with European data protection law». *Tilburg Law School Research Paper* (4, pág. 257 y sig.).

Bloustein, E. J. (1977). «Group Privacy: The Right to Huddle». Rutgers-Cam. L. J. (8, pág. 219 y sig.).

Bloustein, E. J. (1978). *Individual and Group Privacy*. New Brunswick: Transaction Books (pág. 123 y sig.).

Bollier, D. (2010). *The Promise and Perils of Big Data*. Aspen Institute, Communications and Society Program <http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf>

Böröcz, I. (2016). «Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras». *European Data Protection Law Review'*. (2(4), págs. 467-480).

Burnbaum, B. (2013). *Insurers' Use of Credit Scoring for Homeowners Insurance in Ohio: A Report to the Ohio Civil Rights Commission* <https://www.researchgate.net/publication/265217840_Insurers'_

Use_of_Credit_Scoring_for_Homeowners_Insurance_In_Ohio_A_Report_to_the_Ohio_Civil_Rights_Commission>.

Bygrave, L. A. (2002). «Data Protection Law. Approaching Its Rationale, Logic and Limits». *The Hague-New York, Kluwer Law International* (pág. 175 y sig.).

Bygrave, L. A. (2001). «Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling». *Computer Law & Security Rew* (17, 1, pág. 17 y sig.).

Cafaggi, F. (1998). «Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali». *Danno resp*. (pág. 619 y sig.).

Cate, F. H.; Mayer-Schönberger, V. (2013). *Data Use and Impact. Global Workshop*. The Center for Information Policy Research and The Center for Applied Cybersecurity Research, Indiana University.

Cate, F. H.; Mayer-Schönberger, V. (2013). «Notice and consent in a world of Big Data». *Int'l. Data Privacy L*. (3, pág. 67 y sig.).

Citron, D. K.; Pasquale, F. (2014). «The Scored Society: Due Process For Automated Predictions». *Wash. L. Rev.* (89, pág. 1 y sig.).

CNIL (2012). «Measures for the privacy risk treatment». <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf>. Acceso: 25 de febrero de 2017.

CNIL (2015). «Privacy Impact Assessment (PIA). Methodology (how to carry out a PIA)». <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>. Acceso: 25 de febrero de 2017.

CNIL (2015). «Privacy Impact Assessment (PIA). Tools (templates and knowledge bases)» <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>. Acceso: 25 de febrero de 2017.

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2017). *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data* <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>.

Costa, L. (2012). «Privacy and the precautionary principle». *Computer Law & Security Rew.* (28 (1), pág. 14 y sig.).

Crawford, K. (2013). «The Hidden Biases in Big Data». *Harv. Bus. Rev.* <https://hbr.org/2013/04/the-hidden-biases-in-big-data>.

Crawford, K.; Faleiros, G.; Luers, A.; Meier, P.; Perlich, C.; Thorp, J. (2013). *Big Data, Communities and Ethical Resilience: A Framework for Action* <http://www.rockefellerfoundation.org/app/uploads/71b4c457-cdb7-47ec-81a9-a617c956e6af.pdf>.

Cuffaro, V. (2007). Il principio di protezione dei dati». En: V. Cuffaro, R. D'Orazio, V. Ricciuto. *Il codice di trattamento dei dati personali*. G. Giappichelli Editore.

Cuffaro, V.; Ricciuto, V.; Zeno-Zencovich, V. (eds). (1998). *Trattamento dei dati e tutela della persona*. Milano: Giuffrè.

de Montjoye, Y-A.; Radaelli, L.; Kumar Singh, V.; «Sandy» Pentland, A. (2015). «Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata». *Science* (347, 6221, págs. 536-539).

Dixon, P.; Gellman, B. (2014). «The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future». *World Privacy Forum Report* <http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf>.

Ellis, E.; Watson, P. (2015). *EU Anti-Discrimination Law*. Oxford: Oxford University Press.

European Commission (2013). *Developing Anti-Discrimination Law in Europe. The 28 EU Member States, the Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Norway and Turkey compared* <http://www.non-discrimination.net/content/media/Developing Anti-Discrimination Law in Europe EN 29042014 WEB.pdf>.

European Data Protection Supervisor (2015). «Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability» <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf>. Acceso: 12 de febrero de 2017.

European Parliament (2017). «European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225 (INI))» <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//EN&language=EN>. Acceso: 16 de marzo de 2017.

European Parliament (2013). «The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens» <http://info.publicintelligence.net/EU-NSA-Surveillance.pdf

European Parliament (2013). «National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law» <http://www.europarl.europa.eu/committees/it/libe/studiesdownload.html?languageDocument=EN&file=98290. European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs

European Parliament (2013). «Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy» <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN>.

Executive Office of the President of the United States-Council of Economic Advisers (2015). *Big Data Differential Pricing* <https://obamawhitehouse.archives.gov/blog/2015/02/06/economics-big-data-and-differential-pricing>

Federal Trade Commission, (2014). *Data Brokers: A Call for Transparency and Accountability* <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

Ferguson, A. G. (2012). «Predictive Policing: The Future of Reasonable Suspicion». *Emory L. J.* (62(2), pág. 259 y sig.).

Gambaro, A. (1985). «Le banche dati e i limiti della legge». *Quadrimestre* (pág. 524 y sig.).

Giannantonio, E. (1999). «Dati personali (tutela dei)». En: *Enciclopedia del diritto* Milano (pág. 483 y sig.).

Golle, P. (2006). «Revisiting the uniqueness of simple demographics in the US population». En: A. Juels (curador). *Proc. 5th ACM workshop on Privacy in electronic society*. New York: ACM.

Gonçalves, M. E. (2017). «The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward». *Inf. & Comm. Tech. Law* (pág. 20) <http://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1295838?journalCode=cict20>.

Hildebrandt, M. (2006). «Profiling: From Data to Knowledge. The challenges of a crucial technology». *Datenschutz und Datensicherheit* (30(9), pág. 548 y sig.).

Lerman, J. (2013). «Big Data and Its Exclusions». *Stan. L. Rev. Online* (66, pág. 55 y sig.).

Lessig, L. (1999). *Code: and other laws of cyberspace*. New York, N. Y.: Basic Books.

Losano, M. G. (1981). *Corso di informatica giuridica, II*. Milano: Unicopli.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press (pág. 83).

Mantelero, A. (2007). *Il costo della privacy tra valore della persona e ragione d'impresa*. Milano: Giuffrè.

Mantelero, A. (2013). «Competitive value of data protection: the impact of data protection regulation on online behaviour». *Int'l Data Privacy L* (3(4), pág. 234).

Mantelero, A. (2014). «The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics». *Computer Law and Security Review* (30(6), pág. 643 y sig.).

Mantelero, A. (2014). «Toward a New Approach to Data Protection in the Big Data Era». En: U. Gasser, J. Zittrain, R. Faris, R. Heacock Jones (curadores). *Internet Monitor 2014: Reflections on the Digital World*. Cambridge (MA): Berkman Center for Internet and Society at Harvard University (pág. 84 y sig.).

Mantelero, A. (2015). «Data protection, e-ticketing, and intelligent systems for public transport». *Int'l. Data Privacy L* (5(4), pág. 309 y sig.).

Mantelero, A. (2016). «Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection». *Computer Law & Security Rew* (32(2), pág. 238 y sig.).

Mantelero, A. (2017). «From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era». En: L. Taylor, B. van der Sloot, L. Floridi (eds). *Group Privacy: New Challenges of Data Technologies*. Springer.

Mantelero, A.; Vaciago, G. (2014). «Social media and big data». En: B. Akhgar, A. Staniforth, F. Bosco (curadores). *Cyber Crime & Cyber Terrorism. Investigator's Handbook*. Waltham (MA): Elsevier (pág. 175 y sig.).

Mayer-Schönberger, V. (1997). «Generational development of data protection in Europe?». En: P. E. Agre, M. Rotenberg (eds). *Technology and privacy: The new landscape*. Cambridge (MA): MIT Press.

Mayer-Schönberger, V.; Padova, Y. (2016). «Regime Change? Enabling Big Data through Europe's Data Protection Regulation». *Colum. Sci. & Tech. L. Rev.* (Vol. XVII, pág. 315 y sig.).

Mayer-Schönberger, V.; Cukier, K. (2013). *Big Data. A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

Messinetti, D. (1998). «Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali». *Riv. crit. dir. priv.* (pág. 350 y sig.).

Moerel, L. (2014). *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*. Tilburg: Tilburg University Press <http://www.debrauw.com/wp-content/uploads/NEWS-PUBLICATIONS/Moerel_oratie.pdf>.

Moerel, L.; Prins, C. (2016). *Privacy for the homo digitalis. Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things* (pág. 43 y sigs. y 75 y sigs) <https://ssrn.com/abstract=2784123>.

Narayanan, A.; Felten, E. W. (2016). *No silver bullet: De-identification still doesn't work* <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.

Narayanan, A.; Huey, J.; Felten, E. W. (2016). «A Precautionary Approach to Big Data Privacy». En: S. Gutwirth, R. Leenes, P. De Hert (curadores). *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*. Dordrecht: Springer (pág. 357 y sig.).

Navarretta, E. (1999). «Commento sub art. 29, comma 9°, in Tutela della Privacy. Commentario alla L. 31 dicembre 1996, n. 675». En: C. M. Bianca, F. D. Busnelli (a cura di). *Le Nuove leggi civile commentate*. Padova. (n. 2-3, pág. 338 y sig.).

Newman, D. G. (2004). «Collective Interests and Collective Rights». *American Journal of Jurisprudence* (49(1), pág. 127 y sig.).

Nissenbaum, H. (2010). *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press (pág. 231).

Ohm, P. (2010). «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization». *UCLA L. Rev.* (57, pág. 1701 y sig.).

Orestano, A. (2003). «La circolazione dei dati personali». En: Pardolesi, R. *Il diritto alla riservatezza e circolazione dei dati personali, II*. Milano: Giuffrè.

Paparrizos, J.; White, R.W.; Horvitz, E. (2016). «Screening for Pancreatic Adenocarcinoma using Signals from Web Search Logs: Feasibility Study and Results». *Journal of Oncology Practice* (12(8), pág. 737 y sig.).

Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge (MA): Harvard University Press.

Peña Gangadharan, S.; Eubanks, V.; Barocas, S. (2014). *Data and Discrimination: Collective Essays*. Open Technology Institute and New America <http://www.newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL>.

Perry, W.L.; McInnis, B.; Price, C. C.; Smith, S. C.; Hollywood, J. S. (2013). *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*. The RAND Corporation <http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf>.

Pieters, W. (2011). «Security and Privacy in the Clouds: A Bird's Eye View». En: S. Gutwirth, Y. Poullet, P. de Hert, R. Leenes (curadores). *Computers, Privacy and Data Protection: an Element of Choice*. Dordrecht: Springer (pág. 455).

Raab, C.; Wright, D. (2012). «Surveillance: Extending the Limits of Privacy Impact Assessment». En: D. Wright, P. De Hert (curadores). *Privacy Impact Assessment* Dordrecht-New York: Springer (pág. 364).

Rauhofer, J. (2014). «Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age». *University of Edinburgh School of Law, Research Paper Series* (2014/06, pág. 5 y sigs.) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2389981>.

Resta, G. (2000). «Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali». *Riv. crit. dir. priv.* (pág. 310 y sig.).

Ricciuto, V. (2007). *Il codice del trattamento dei dati personali*. Torino: Giappichelli (pág. 11 y sigs.).

Richards, N. M.; King, J. H. (2013). «Three Paradoxes of Big Data». *Stan. L. Rev. Online* (66, pág. 43).

Rieke, A.; Robinson, D.; Yu, H. (2014). *Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology* <http://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf>.

Rodotà, S. (1991). «Privacy e costruzione della sfera privata. Ipotesi e prospettive». *Pol. dir.* (pág. 521 y sig.).

Rodotà, S. (1995). *Tecnologia e diritti*. Bologna: Il Mulino.

Rodotà, S. (1973). *Elaboratori elettronici e controllo sociale*. Bologna.

Rodotà, S. (1997). *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*. Roma-Bari: Laterza (pág. 134 y sig.).

Rosenblat, A.; Randhava, R.; Boyd, D.; Peña Gangadharan, S.; Yu, C. (2014). *Data & Civil Rights: Consumer Finance Primer* <http://www.datacivilrights.org/pubs/2014-1030/Finance.pdf>.

Rubinstein, I. S. (2013). «Big Data: The End of Privacy or a New Beginning?». *Int'l. Data Privacy L* (3(2), pág. 74 y sig.).

Samuelson, P. (2000). «Privacy as Intellectual Property?». *Stan. L. Rev* (52(5), pág. 1125).

Schreurs, W.; Hildebrandt, M.; Kindt, E.; Vanfleteren, M. (2010). «Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector». En: M. Hildebrandt, S. Gutwirth (curadores). *Profiling the European Citizen. Cross-Disciplinary Perspective*. Dordrecht: Springer (pág. 241 y sig.).

Shelley-Egan, C. *et al.* (2014). *SATORI Deliverable D2.1 Report (handbook) of participatory processes* <http://satoriproject.eu/work_packages/dialogue-and-participation/>. Acceso: 15 de febrero de 2017.

Sica, S. (2001). «Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica». *Riv. dir. civ.* (II, pág. 629 y sig.).

Sweeney, L. (2013). «Discrimination in Online Ad Delivery». *Communications of the ACM* (56(5), pág. 44 y sig.).

Sweeney, L. (2000). «Foundations of Privacy Protection from a Computer Science Perspective». *Proc. Joint Statistical Meeting*. Indianapolis: AAAS <http://dataprivacylab.org/projects/disclosurecontrol/paper1.pdf>

Sweeney, L. (2000). *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University <http://dataprivacylab.org/projects/identifiability/paper1.pdf>.

Tene, O.; Polonetsky, J. (2012). «Privacy in the Age of Big Data. A Time for Big Decisions». *Stan. L. Rev. Online* (64, págs. 63–69) <http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf>. Acceso: 14 de octubre de 2016.

The White House, Executive Office of the President (2016). *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Acceso: 4 de marzo de 2017.

The White House, Executive Office of the President (2014). *Big Data: Seizing Opportunities, Preserving Values* <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf>.

Trilateral Research & Consulting (2013). *Privacy impact assessment and risk management. Report for the Information Commissioner's Office* <https://ico.org.uk/media/1042196/trilateral-full-report.pdf>. Acceso: 25 de febrero de 2017.

United States General Accounting Office (2011). *Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information* (pág. 68 y sig.) <http://www.gao.gov/assets/210/201699.pdf>. Acceso: 14 de diciembre de 2013.

Van Brakel, R.; De Hert, P. (2011). «Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies». *Journal of Police Studies* (20(3), pág. 163 y sig.). KDD: The Challenge to Individualism». *Ethics and Information Technology* (1, pág. 275 y sig.).

Vedder, A. (1997). «Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations». En: G. Moore (curador).*Business Ethics: Principles and Practice*. Warwick (RI): Business Education Publishers (pág. 215 y sig.).

Vedder, A.; Laurens Naudts, L. (2017). «Accountability for the use of algorithms in a big data environment». *International Review of Law, Computers & Technology* <http://dx.doi.org/10.1080/13600869.2017.1298547>. Acceso: 2 de mayo de 2017.

Westin, A. F. (1970). *Privacy and Freedom*. New York: Atheneum (pág. 42 y sig.).

Whitman, J. Q. (2017). «The Two Western Cultures of Privacy: Dignity versus Liberty». *Yale L. J.* (113, pág. 1151 y sig.).

Wright, D. (2011). «A framework for the ethical impact assessment of information technology». *Ethics Inf Technol* (13(3), pág. 222).

Wright, D.; Raab, C. (2014). «Privacy principles, risks and harms». *International Review of Law, Computers & Technology* (28(3), págs. 277-298).

Zarsky, T. Z. (2013). «Transparent Predictions». *U. Ill. L. Rev* (4, pág. 1510 y sigs.).

Zeno-Zencovich, V. (1995). «Personalità (diritti della)». En:*Dig. Disc. Priv.*. Torino (Sez. Civ., vol. XIII, pág. 430 y sigs.).