¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca*

Ricardo Morte Ferrer
Abogado,
Doctorando en Filosofía
Universidad de Granada.
Proyecto KONTUZ!
ricardo63@autistici.org

Privacy in the Times of Big Data, IoT, Wearables…? Yes, More than Ever

Resumen: Desde hace ya algún tiempo, de forma general cabría decir que con el desarrollo de Internet, y de una forma especialmente intensa desde la aparición del Cloud Computing y el incremento de la importancia de las redes sociales, parece haber una tendencia a afirmar que hemos entrado en una era post Protección de Datos/ Privacidad. Esa tendencia para haberse intensificado con la última remesa de nuevas tecnologías mencionadas en el título de este trabajo, motivo por el cual consideramos necesario hacer una breve revisión de la evolución histórica en materia de Protección de Datos/Privacidad, aclarar el verdadero significado de estos conceptos y explicar el motivo por el que creemos que no solo no han perdido vigencia, sino que incluso son más importantes que nunca, especialmente por su capacidad de proteger a individuos especialmente vulnerables, revisando no solo aspectos jurídicos, sino también éticos.

Palabras clave: Protección de Datos, Privacidad, Big Data, ética, vulnerabilidad

Abstract: For some time now, generally speaking we could say since the development of Internet, and specially with the appearance of Cloud Computing and the increasing importance of social networks, it seems to be a tendency to believe that we are in a post-Privacy age. This tendency looks even more intense after the last package of new technologies mentioned in the title of this paper, that is the reason why we think that it is necessary to make a brief review of the historical development of Privacy, to clear what Privacy really means and to explain why this concept not only has not lost its current value, it is even more important than ever, particularly because of its capability to protect vulnerable subjects. We will make this review from both a legal and an ethical point of view.

Keywords: Privacy, Big Data, ethics, vulnerability

ISSN 1989-7022

1. Introducción

La evolución de las tecnologías de la información y la comunicación (TIC) ha experimentado una aceleración impresionante con el desarrollo de Internet. El mencionado desarrollo ha traído consigo la aparición de diferentes empresas que han alcanzado un volumen y un grado de poder inimaginables hace algún tiempo. Las cinco principales, especialmente en lo que afecta al tema que nos ocupa en este trabajo, son las que yo llamo "los cinco jinetes del apocalipsis de la Protección de Datos": Amazon, Apple, Facebook, Google y Microsoft. Algunos creemos que ese grado de poder es realmente excesivo y que esas empresas muestran en muchas ocasiones tendencias totalitarias, o como mínimo monopolísticas e ilegales. Ese tema sería más adecuado para otro trabajo, pero en el que nos ocupa nos servirá para demostrar la importancia de la Protección de Datos/Privacidad como instrumento esencial de protección de los sujetos afectados en las relaciones asimétricas de poder en las que se ve inmerso en sus relaciones con esas empresas y con otras organizaciones, como por

* Este trabajo se ha realizado en el marco del proyecto de investigación KONTUZ!: "Responsabilidad causal de la comisión por omisión: Una dilucidación ético-jurídica de los problemas de la inacción indebida" (MINECO FFI2014-53926-R)

Received: 30/04/2017
Accepted: 20/05/2017

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

ejemplo los estados y sus fuerzas de seguridad, empresas de seguros, empresas financieras, etc.

Para poder comprender mejor la situación, parece necesario hacer una revisión histórica de la evolución en materia de Protección de Datos, especialmente porque parece existir una sensación según la cual este es un tema nuevo que ha llegado con la era de Internet y de las nuevas tecnologías. Como veremos a continuación esa idea es equivocada.

También será necesario aclarar de qué hablamos cuando hablamos de Protección de Datos/Privacidad. El mero hecho de recurrir a dos términos diferentes ya deja claro que es una cuestión esencial. Para facilitar la lectura del trabajo y en parte también debido a que en la actualidad el término que más se utiliza es el de privacidad, a partir de este momento recurriremos al mismo, salvo cuando hagamos referencia a normativas especiales o a épocas en las que el otro término era el dominante.

2. Breve revisión histórica

En esta revisión histórica nos centraremos en el desarrollo legislativo en Europa y en EEUU, así como en algunos trabajos teóricos sobre el tema en esas dos zonas. Otras zonas, como Latinoamérica han tenido una evolución algo distinta, entre otras cosas por motivos históricos con la existencia de dictaduras que han hecho que se privilegiara el desarrollo en materia de transparencia y se dejara el tema de la privacidad algo de lado.

Como he mencionado anteriormente, el tema de la privacidad no es nuevo, ni ha llegado con Internet. Si la revisión histórica fuera realmente profunda podríamos encontrar diferentes variaciones del tema ya en la antigüedad, pero para el enfoque escogido para este trabajo empezaremos la revisión a finales del Siglo XIX.

a) En 1890 se publica el artículo "*The Right to Privacy*" (Warren & Brandeis, 1890). Es curioso observar que el primer trabajo profundo en materia de privacidad se publicara en EEUU, especialmente porque el desarrollo posterior en la materia en ese país no ha seguido el camino que cabía esperar después de este inicio. El artículo en cuestión resulta especialmente interesante para este trabajo, porque sus autores, un abogado y un juez que llegó a formar parte del *Supreme*

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

Court, se sintieron motivados a estudiar la privacidad debido al desarrollo de una nueva tecnología que les parecía peligrosa en lo que afecta a la privacidad: la fotografía y su uso indiscriminado por parte de la prensa. En este trabajo los autores identificaban la privacidad con el derecho a que nos dejen tranquilos, o en la versión angloparlante "*right to be let alone*". La situación a la que se enfrentaban los autores es hasta cierto punto similar a la actual, la nueva tecnología se utilizaba para hacer negocio con los datos personales de los sujetos afectados, ignorando su derecho a la privacidad.

b) La siguiente publicación significativa en materia de privacidad aparece también en EEUU, se trata de "*Privacy and Freedom*" (Westin, Alan F., 1967). Westin sienta las bases de lo que hoy en día se entiende, de forma más o menos generalizada, por privacidad al afirmar que los individuos tienen el derecho a decidir qué datos personales puede ser accesible, quien puede acceder a la misma y como deberá almacenarse y distribuirse esa información. Es lo que se conoce como el derecho a la autodeterminación informativa, y llama la atención que Westin fuera capaz de captar los problemas que se podían generar en la materia antes de que existieran ordenadores personales y mucho antes de que apareciera Internet.

c) El siguiente momento histórico relevante no está relacionado con la publicación de un trabajo científico, sino con la aparición de la primera legislación del mundo en materia de privacidad. Se trata de la Ley de Protección de Datos del Land alemán de Hessen(1970)[1] en el marco de la Administración Pública de ese Land, el marco de aplicación también muestra un aspecto importante en la evolución de la privacidad: en ese momento se consideraba que el mayor riesgo provenía del Estado y de sus cuerpos y fuerzas de seguridad.

d) El siguiente momento histórico también está marcado por una ley: la Ley Federal de Protección de Datos alemana (1977)[2]. En esta ley se amplía el campo de aplicación y se marca como objetivo la protección de los datos personales tanto en lo referente a los tratamientos llevados a cabo en el sector público como a los tratamientos organizados por empresas privadas. Esta ley introdujo el principio de "*Verbot mit Erlaubnisvorbehalt* /prohibición con excepción de autorización" según el cual cualquier tratamiento de datos personales está prohibido, salvo que el sujeto afectado haya dado su consentimiento o exista una autorización legal para el tratamiento de datos personales. Este principio está en el núcleo de las regulaciones en materia de privacidad en Europa y es uno de los puntos

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

que los defensores de la afirmación "vivimos en una época postprivacidad" pretenden desvirtuar.

e) En 1983 se puede mencionar el siguiente momento histórico, marcado por la Sentencia del Censo del Tribunal Constitucional Alemán[3], que recoge de forma expresa el Derecho Fundamental a la autodeterminación informativa, en la antes mencionada dirección marcada por Westin en 1967.

f) En 1995 aparece la primera normativa de Protección de Datos a nivel Europeo: la Directiva Europea 95/46/CE de Protección de Datos, que a grandes rasgos aplica a nivel europeo los criterios contenidos en las ya mencionadas normativas alemanas. Cabe resaltar que a día de hoy esta normativa sigue vigente.

g) En 1999 se aprueba en nuestro país la Ley Orgánica 15/1999 de Protección de Datos (LOPD)[4] por medio de la cual se implementa la Directiva Europea mencionada en el punto anterior en la legislación española.

h) En 2007 se aprueba el Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[5].

i) Para el siguiente momento histórico a mencionar, en 2008, hay que volver a Alemania y hacer referencia a la 2008 Sentencia del Tribunal Constitucional Alemán sobre la inviolabilidad de los sistemas informáticos[6].

j) El último, al menos de momento, punto a mencionar, en 2016, es la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[7], que deroga la Directiva Europea anteriormente mencionada y que entrará en vigor el 25.05. 2018. Aunque posteriormente haremos otros comentarios al respecto, cabe mencionar como puntos esenciales un aumento de las multas a aplicar, un intento de armonizar la normativa europea y una introducción de la cultura de la gestión de riesgos en sustitución de la de la aplicación del principio de precaución.

Esta enumeración no pretende ser exhaustiva, sino simplemente dar una imagen panorámica de la evolución en la materia que nos ocupa. Para concretar algo más esa imagen, procederemos a profundizar algo más sobre las dos sentencias del Tribunal Constitucional alemán ya mencionadas.

Han pasado ya más de 30 años desde que ese Tribunal decidió, en el marco de las protestas populares contra el censo, que no era correcto almacenar información sobre

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

los ciudadanos de forma ilimitada. En su sentencia, el Tribunal definió el derecho a la autodeterminación informativa como nuevo derecho fundamental autónomo.

La sentencia, que ha pasado a la historia como la "sentencia del censo" se basaba en un razonamiento que sigue de actualidad en la que podríamos calificar como la era de las redes sociales (y de las tecnologías mencionadas en el título del presente artículo): "El derecho a la autodeterminación informativa presupone, también en el marco de las nuevas tecnologías de la información, que cada individuo pueda decidir de forma libre sobre posibles tratamientos de sus datos, así como de poder actuar en función de los mismos. El derecho a las autodeterminación informativa hace imposible la existencia de un sistema social y legal en el que los ciudadanos no puedan saber quién, qué, cuándo y en qué condiciones dispone de información sobre ellos".

Contra la Ley del Censo se habían presentado diferentes recursos, entre ellos el de Wilhelm Steinmüller (quien en 2007 publicó un breve artículo sobre el origen del derecho a la autodeterminación informativa citado en la bibliografía de este artículo), en el que se desarrollaba el concepto de autodeterminación informativa que posteriormente sirvió de fundamento para la sentencia. Ese recurso también hacía referencia al almacenamiento preventivo de datos, y cabe suponer que esa referencia fue la base para que el Tribunal suprimiera la posibilidad de comparar los datos del censo con el número de viviendas, ya que eso habría posibilitado una "repersonalización" de los datos estadísticos.

La otra sentencia a mencionar es la del Tribunal Constitucional alemán en 2008, que es considerada como la fuente del nuevo "derecho a la integridad y confidencialidad de los sistemas informáticos", y que supone una concreción en la definición de la protección de datos frente a las nuevas tecnologías. La sentencia responde a un recurso presentado contra la reforma de la ley de los servicios de inteligencia del Land de Renania del Norte Westfalia, en virtud de la cual se permitía expresamente que esos servicios pudieran utilizar de forma secreta troyanos para espiar los ordenadores de cualquier sospechoso, lo cual significa entrar en el ordenador, reunir toda la información encontrada y analizarla posteriormente. El Tribunal consideró la reforma como inconstitucional y configuró el nuevo derecho ya mencionado.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

Estas dos sentencias adquieren mayor importancia en relación con la próxima entrada en vigor del nuevo Reglamento Europeo de Protección de Datos, ya que esa nueva normativa cerrará el acceso de los ciudadanos a recursos de amparo en materia de protección de datos antes los tribunales constitucionales de los países miembros. Eso es especialmente grave en Alemania, donde el Tribunal Constitucional ha sido especialmente activo en la materia. Ese problema es más grave de lo que pueda parecer en principio, ya que la Unión Europea carece de un tribunal equivalente capaz de ofrecer una protección adecuada a los ciudadanos.

3. ¿De qué hablamos cuando hablamos de privacidad?

Como hemos mencionado anteriormente, existe una cierta confusión en lo que afecta a la terminología utilizada en el tema que estamos estudiando. Hay que empezar por aclarar que el término Protección de Datos, pese a que personalmente nos guste más que el de privacidad, es relativamente desafortunado, ya que da la sensación de proteger a los datos personales como tales. En realidad lo que se protege son las personas con las que esos datos están relacionados: los sujetos afectados. Los datos como tales son protegidos por la seguridad de la información.

Aparte de la aclaración ya mencionada, cabe recordar que la terminología que se utilice tiene consecuencias en función de quien reciba la información: el típico problema emisor/receptor. De nuevo recurriremos a una breve lista que puede dar una imagen aproximada de la situación actual:

a) En nuestro país al hablar de protección de datos se relaciona con los problemas burocráticos que la aplicación de la ley puede suponer para algunas empresas. Si bien el problema no es tan grave como en ocasiones se presenta, cabe recordar que la escalabilidad de la aplicación de la ley es uno de los problemas a tener en cuenta. El que algunos juristas consideren el derecho a la autodeterminación informativa como un derecho de cuarta generación no ayuda a valorar ese derecho de la forma adecuada.

b) Cuando se habla de privacidad en muchas ocasiones se limita ese concepto a la intimidad y al ya mencionado derecho a ser dejado tranquilo/ *right to be let alone*, sin entender la extensión que el concepto tiene en el idioma inglés, por ejemplo en relación con el ya mencionado planteamiento de Westin.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

c) Cuando recurrimos a una traducción directa de protección de datos al inglés (*data protection*) nuestros interlocutores seguramente lo relacionarán con la seguridad de la información.

Aunque se podrían incluir otros aspectos, creo que los ya mencionados puntos dan una idea clara del problema.

Cuando nosotros (y otros autores como Rost, 2013) hablamos de privacidad hacemos referencia a un problema de relaciones de poder. En nuestra opinión la privacidad controla los tratamientos de datos y las comunicaciones en las relaciones asimétricas de poder entre organizaciones y sujetos afectados. A continuación aportamos una imagen que refleja muy bien este planteamiento.

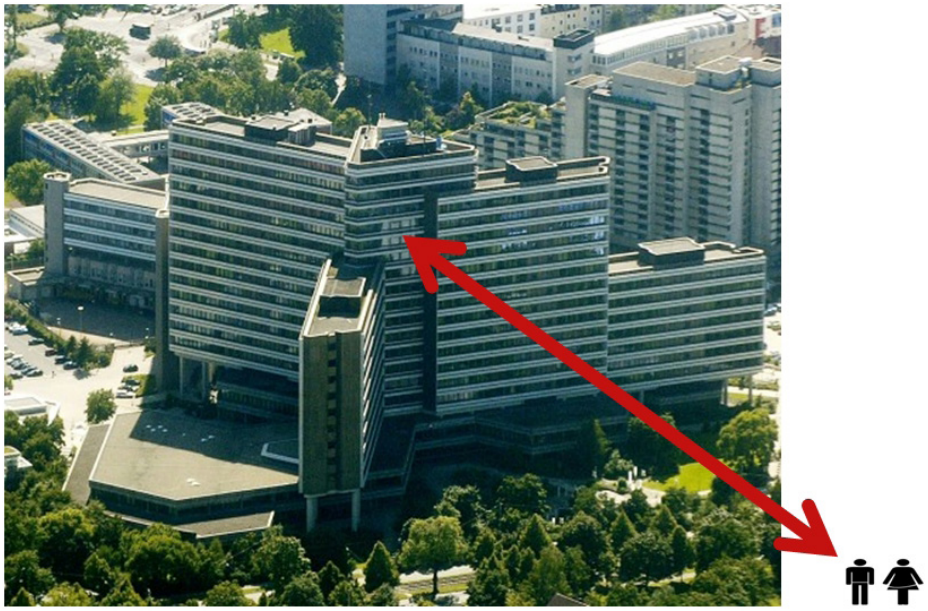

Figura 1. Explicación privacidad

Quizás sea necesario aclarar a qué nos referimos cuando hablamos de relaciones asimétricas de poder. Un ejemplo claro es el de la relación entre las administraciones públicas y los ciudadanos, esa relación está en el inicio del desarrollo de las normativas de privacidad para proteger a los sujetos afectados frente a un exceso de poder del Estado y de sus fuerzas y cuerpos de seguridad. En la actualidad un ejemplo claro puede ser el de la relación existente entre Facebook y sus usuarios, ya que cada vez más parece que el tener una cuenta de esa red social es imprescindible, y por otra parte los usuarios no disponen de información suficiente para tomar decisiones referentes a su relación con Facebook. Por poner un ejemplo, el consentimiento otorgado por los usuarios no es informado, en parte porque la mayoría no lee a

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

fondo las condiciones, pero también porque si las leyeran no dispondrían de toda la información referente a como la red social utiliza sus datos. Además conviene mencionar que en la actualidad el no disponer de cuenta de Facebook puede suponer problemas, por ejemplo en el mundo laboral.

4. Los objetivos de protección

A continuación haremos una breve revisión de lo que se conoce como objetivos de protección tanto en el campo de la seguridad informática como en el de la protección de datos. Estos objetivos de protección nos servirán para analizar posteriormente un problema concreto que reflejará de forma especialmente clara la vigencia de la privacidad.

Los objetivos de protección han jugado un papel básico en la organización de sistemas técnicos cuya seguridad debe ser garantizada desde finales de los años 80. Los objetivos de protección clásicos de la seguridad de los datos son:

- Disponibilidad, este objetivo refleja la exigencia de que los datos personales estén disponibles para ser utilizados de forma adecuada en el proceso para ellos previsto. Para ello deben ser accesibles para las personas previstas y se les deben poder aplicar los métodos previstos para su tratamiento, eso incluye, entre otras cosas, que los métodos sean aplicables al formato en el que los datos están disponibles. La disponibilidad incluye que los datos sean localizables, que los sistemas implicados los puedan presentar de forma adecuada y que esa presentación sea semánticamente comprensible.
- Integridad, en este caso el objetivo de protección resalta como exigencia que los procesos y sistemas informáticos sean capaces de mantener las características que son esenciales para la realización de las funciones imprescindibles para alcanzar la finalidad establecida y, al mismo tiempo, que los datos tratados permanezcan indemnes, completos y actuales. Posibles efectos secundarios deben ser evitados o tenidos en cuenta y tratados. Este objetivo de protección exige que entre las exigencias y la realidad haya una garantía suficiente, tanto en los detalles técnicos como en lo que afecta al tratamiento en general y su ajuste a las finalidades establecidas.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

- Confidencialidad, este objetivo de protección recoge como exigencia que nadie pueda acceder a los datos personales sin autorización. En ocasiones el acceso a los datos permite que el sujeto afectado sea identificado porque el contexto en el que los datos son almacenados permite sacar conclusiones sobre ese sujeto. Cuando nos referimos a personas no autorizadas, eso no significa que se trate necesariamente de terceros ajenos a la organización, que pueden actuar con intenciones criminales o de otro tipo, sino que puede tratarse también de empleados de servicios técnicos que para prestar esos servicios no precisan de acceso a los datos personales, o de personas activas en departamentos de la organización que no tienen ninguna relación con un determinado proceso o con el sujeto afectado.

Estos tres objetivos de protección han sido aceptados por los responsables por iniciativa propia, ya que los consideraban como necesarios para su propia protección sin que existiera una normativa legal que les obligara a aplicarlos. En un principio fueron formulados para su aplicación en el ámbito de la seguridad informática y describe exigencias para un operativo seguro, especialmente en lo que afecta a procesos en el marco de organizaciones y en relación con su negocio o administración. Esas organizaciones tienen que proteger sus procesos, independientemente de que los posibles atacantes sean personas ajenas a ellas miembros de las mismas.

En función de la normativa aplicable, el nivel de exigencia en lo que afecta a estos objetivos de protección es variable. Por ejemplo, en el ámbito privado el objetivo de la disponibilidad se cumple siempre que los datos no sean destruidos ni se pierdan.

Aparte de los ya mencionados objetivos de protección originados en el campo de la seguridad informática, se han desarrollado otros objetivos cuyo interés se centra en la Protección de Datos basados en normativa existente en la materia y a partir de los cuales se pueden derivar medidas técnicas y organizativas. Desde el punto de vista de la normativa de Protección de Datos, las organizaciones deben proteger sus procesos de posibles ataques, siempre que esos procesos afecten a datos de carácter personal. Los objetivos de protección de la Protección de Datos precisan, en comparación con los objetivos de protección de la seguridad informática, de un grado de comprensión más amplio, ya que la Protección de Datos tiene en cuenta una perspectiva de protección adicional, al tener en cuenta los riesgos que las actividades de la organización en sí mismas pueden originar para el sujeto afectado,

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

tanto en el ámbito de sus procesos de negocio/administración como fuera de ellos. Desde el punto de vista metodológico eso significa que no sólo una persona debe demostrar ante una organización que es de confianza, sino que la organización debe ser capaz de demostrar frente a una persona que es de confianza. Por ese motivo es preciso establecer objetivos de protección que garanticen la protección de los sujetos afectados frente a diferentes tipos de organizaciones.

Estos objetivos de protección específicos de la Protección de Datos, cuya finalidad es la protección del sujeto afectado, son:

- No encadenabilidad, refleja la exigencia de que los datos sólo sean tratados y valorados para la finalidad para la que fueron recogidos.
- Transparencia, requiere que, aunque en diferentes niveles, tanto el sujeto afectado, como el responsable de los sistemas y posibles autoridades de control puedan reconocer qué datos y para qué finalidad han sido recogidos y tratados en un proceso, que sistemas y procesos han sido utilizados, en qué dirección y para qué fines fluyen los datos y quien es el responsable legal de los datos y sistemas en las diferentes fases de un tratamiento de datos. La transferencia es imprescindible para el control y dirección de los datos, procesos y sistemas desde su inicio hasta su cancelación, y un requisito previo para que un tratamiento de datos sea legítimo y, en caso de necesidad, los sujetos afectados puedan otorgar su consentimiento.

  La transparencia de un tratamiento de datos en su conjunto y de las partes implicadas puede permitir que especialmente los sujetos afectados y las autoridades de control puedan detectar posibles fallos y exigir que se lleven a cabo las modificaciones necesarias para suprimirlos.
- Capacidad de intervenir, exige que el sujeto afectado pueda ejercer de forma efectiva sus derechos ARCO (en nuestro país se mencionan de esa forma los derechos de acceso, rectificación, cancelación y oposición) en cualquier momento, y que el responsable está obligado a tomar las medidas necesarias para hacer efectivos esos derechos. Para alcanzar este objetivo debe ser posible modificar el tratamiento de datos en cualquier momento y en cualquiera de sus fases, desde la recogida de los datos hasta su cancelación.

En principio conjuntos o paquetes de datos son adecuados para ser utilizados para otros fines y para ser combinados con otros datos, posiblemente de acceso

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

público. Cuanto mayores son esos paquetes de datos y cuanto más información aporten, mayor es el interés que despiertan. Desde el punto de vista legal, esas combinaciones sólo son aceptables en condiciones muy especiales y estrictamente fijadas. La normativa de Protección de Datos exige que el tratamiento sea separado en función de las finalidades y/o que los datos sean almacenados de forma separada en función de la finalidad para la que son tratados.

Al igual que sucede con los objetivos de protección clásicos, los de la Protección de Datos también están influenciados por la normativa que les es aplicable y por el ámbito en el que deben ser aplicados. Por ejemplo, en el ámbito privado la transparencia no es imprescindible en cada caso de uso de los datos en el campo de actuación de un responsable, salvo que ese uso suponga una modificación de los datos.

5. Análisis de la problemática del Big Data como ejemplo de la vigencia de la privacidad

Parece necesario empezar por intentar explicar de forma breve qué es el Big Data. Aunque se han publicado diferentes obras sobre el tema, incluyendo algunas que califican al Big Data como "la revolución que cambiará nuestras vidas" (Mayer Schönberger y Cukier, 2013), a día de hoy no existe una definición generalmente aceptada. Se puede afirmar que Big Data hace referencia a una nueva tecnología, o desarrollo de tecnologías ya existentes, capaz de tratar de una forma cada vez más rápida grandes cantidades de datos y que puede suponer un cambio de paradigma en diferentes campos del conocimiento (de hecho, en algunos campos parece haberlo conseguido). Ese cambio de paradigma se centra en el abandono de la causalidad como criterio central y su sustitución por la correlación. Conviene mencionar que hay autores que discrepan de esa opinión y que incluso han calificado la época del Big Data como una "época sin razón" y que han comparado el boom en torno al Big Data con el que se produjo desde el Siglo XVII en torno a la estadística (Han, Byung Chul, 2014).

Es evidente que uno de los motivos esenciales por los que existe tanta atención, y tanta expectación, en torno al Big Data se debe a su potencial desde el punto de vista económico. De todas formas, en nuestra opinión es evidente que esta tecnología también plantea diferentes problemas. Especialmente después de las filtraciones

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

aportadas por Edward Snowden es evidente que esta tecnología tiene un lado oscuro y que supone nuevos peligros en un mundo cada vez más interconectado. Las posibilidades que ofrece el tratamiento masivo de datos abre nuevas oportunidades en el mundo de la ciencia y de los negocios, pero presenta nuevos peligros en torno a un posible uso inadecuado de esos datos.

Las aplicaciones de Big Data tiene como objetivo el prever posibles pautas de comportamiento de una persona o grupo de personas. Algunos ejemplos

a) Analizar la posibilidad de un comportamiento determinado en relación con diferentes tipos de contratos (*scoring*).

b) Acumular datos en principio inconexos con el fin de crear un perfil detallado de una persona o de un grupo de personas (*profiling*).

c) Valorar diferentes características de una persona, como pueden ser su estado de salud, sus gustos o su fiabilidad (*personalizing*).

d) Seguir a una persona en base al rastro que deja, por ejemplo en Internet (*tracking*).

Parece evidente que estas actividades traen consigo diferentes riesgos, algunos autores hablan de una "dictadura *smart*" (Weltzer, 2016) en base a esos riesgos y al grado de desarrollo que algunas tecnologías están alcanzando. Conviene recordar que muchas de esas tecnologías han sido ya implementadas sin que se hayan llevado a cabo estudios previos sobre los posibles peligros para los derechos fundamentales y sin que existan políticas adecuadas de seguridad informática para esas nuevas aplicaciones y productos.

Antes de proceder a realizar un breve análisis basado en los objetivos de protección, como ya hemos anunciado, conviene recordar un principio que hemos mencionado en la revisión histórica: el de prohibición con excepción de autorización. De acuerdo con ese principio cualquier tratamiento de datos está prohibido salvo que el sujeto afectado haya dado su consentimiento para el mismo o que exista una normativa que lo autorice. Al respecto conviene mencionar que hay autores que cuestionan que el consentimiento sea un instrumento válido en situaciones asimétricas de poder (Kamp y Rost, 2013) y que para que un consentimiento sea válido debe ser específico, libre e informado. Las explicaciones que hemos dado hasta hora sobre el Big Data deberían ser suficientes para demostrar que en el campo del Big Data el consentimiento no es el instrumento adecuado para dar base legal al

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

tratamiento de datos, ya que el sujeto afectado normalmente no es consciente de la existencia del tratamiento de sus datos personales. Estos y otros problemas han sido tratados por Thilo Weichert, anterior director del *Unabhängiges Landeszentrum für Datenschutz* en Kiel[8].

A continuación realizaremos un breve chequeo del Big Data en base a los objetivos de protección:

a) Disponibilidad: es un tema a valorar especialmente en análisis realizados en tiempo real.

b) Integridad: dependiendo de cuál sea la fuente en la que se hayan obtenido los datos, por ejemplo en Internet, puede suponer un problema.

c) Confidencialidad: solo se podría alcanzar este objetivo de protección mediante una anonimización absoluta de los datos. Cabe recordar que es muy difícil alcanzar una anonimización absoluta de los datos, ya que nuevas tecnologías podrían hacer posible una repersonalización de los datos.

d) No encadenabilidad: por la naturaleza misma del Big Data es imposible alcanzar ese objetivo.

e) Transparencia: en este ámbito las empresas activas en el campo del Big Data suelen excusarse haciendo referencia al secreto industrial. Desde el punto de vista del sujeto afectado es evidente que no es alcanzable ya que, a diferencia de lo que sucede en los tratamientos "tradicionales", él no es consciente de la existencia del tratamiento.

f) Capacidad de intervenir: no es alcanzable, y de momento las empresas implicadas no han mostrado ningún interés en tratar el tema

En nuestra opinión, esta breve revisión del tema del Big Data demuestra la vigencia de la privacidad y del instrumento esencial para su protección: el derecho fundamental a la autodeterminación informativa en el momento actual.

6. Conclusiones

En nuestra opinión, se hace difícil discutir la vigencia de la privacidad en una época marcada por la aparición constante de nuevas tecnologías que suponen la aparición

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 219-233

de nuevos riesgos para los sujetos afectados y para sus derechos fundamentales. De todas formas también debemos constatar que uno de los problemas esenciales reside en que los sujetos afectados en muchas ocasiones no son conscientes de la existencia de esos riesgos, de hecho en muchas ocasiones son colaboradores esenciales de las empresas que realizan un tratamiento inadecuado de sus datos y que atentan contra sus derechos fundamentales. El ejemplo más claro es el uso de los smartphones y el de redes sociales, como Facebook, que infringen de forma clara la normativa de protección de datos[9].

Se hace necesario valorar de forma adecuada qué nos aportan las nuevas tecnologías y de qué forma se deben implementar controles previos a su entrada en el mercado y en las vidas de los sujetos afectados. No sirve el discurso basado en el criterio "las leyes no se adaptan lo suficientemente rápido a la nueva situación", en la mayoría de los casos las leyes vigentes son aplicables a las nuevas tecnologías y lo único que hace falta es voluntad política para conseguir que se cumplan. El principio de prohibición con excepción de autorización sigue vigente y no es aceptable que las grandes empresas TIC intenten cambiarlo por el de autorización con excepción de prohibición. No se debe interpretar estas afirmaciones como un postulado por la prohibición de las nuevas tecnologías, sino como una advertencia para una implementación prudente de las mismas y por un mantenimiento de la protección de los derechos fundamentales de los ciudadanos.

Es necesario recordar que en las relaciones asimétricas de poder que se presentan en un mundo cada vez más interconectado se presentan situaciones de vulnerabilidad realmente graves para los ciudadanos, el campo de la salud puede ser uno de los ejemplos más claros, tanto por la reutilización de los datos, como por una posibilidad de que personas enfermas sufran consecuencias negativas por el tratamiento de sus datos de salud, un tratamiento que hasta el momento ha sido muy restringido por la normativa vigente en materia de privacidad y por un criterio ético de protección de ese punto central en lo que afecta a los datos de carácter personal. Sirva de ejemplo el que la empresa Acxiom calificara a personas con escasa capacidad económica como "waste" /basura (Han, Byung Chul, 2014) y que algunos autores advierten que uno de los objetivos esenciales de las estructuras de vigilancia continuada es separar lo útil a nivel económico de lo inútil o prescindible (Bauman y Lyon, 2013), conviene recordar que no estamos hablando de cifras o de objetos, sino de personas.

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 219-233

Como punto final quizás convenga recordar que Aristóteles afirmó que la democracia existe cuando las normas son hechas por los indigentes, y no por los propietarios. La mencionada clasificación de las personas llevada a cabo por la empresa Acxiom y las advertencias sobre la finalidad de la vigilancia continuada deberían llevarnos a cuestionar en qué tipo de sociedad vivimos.

Bibliografía

Bauman und Lyon, (2013): Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung. Berlin, Suhrkamp.

Han, Byung-Chul, (2014): Psychopolitik. Neoliberalismus und die neuen Machttechniken. Frankfurt am Main, Fischer.

Kamp, Meike; Rost, Martin, (2013): Kritik an der Einwilligung; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 80-84.

Mayer-Schönberger, V., Cukier, K., (2013): Big Data: A Revolution That Will Transform How We Live, Work and Think. Boston: Houghton Mifflin Harcourt

Rost, Martin, (2013): Zur Soziologie des Datenschutzes; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 85-91.

Warren, S., Brandeis, L., 1890. The Right to Privacy. Boston, Harvard Law Review.

Westin, A.F., 1967: Privacy and Freedom. New York, Athenum.

Weltzer, Harald, (2016): Die smarte Diktatur. Der Angriff auf unsere Freiheit. Frankfurt am Main, Fischer.

Notas

1. https://de.wikipedia.org/wiki/Hessisches_Datenschutzgesetz; localizable el 15.05.2017

2. https://www.datenschutz-wiki.de/BDSG_1977; localizable el 15.05.2017

3. https://openjur.de/u/268440.html; localizable el 15.05.2017

4. http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html; localizable el 15.05.2017

5. http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html; localizable el 15.05.2017

6. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html; localizable el 15.05.2017

7. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679; localizable el 15.05.2017

8. https://www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf localizable el 18.05.2017

9. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3646/6.pdf localizable el 20.05.2017