Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER MONOGRÁFICO XIII CONGRESO MUNDIAL IAB

Datos masivos con privacidad y no contra privacidad

Big Data with Privacy, not against Privacy

YASMINA SOTO *

OBSERVATORI DE BIOÈTICA I DRET DE LA UNIVERSITAT DE BARCELONA

La Revista de Bioética y Derecho se creó en 2004 a iniciativa del Observatorio de Bioética y Derecho (OBD), con el soporte del Máster en Bioética y Derecho de la Universidad de Barcelona: www.bioeticayderecho.ub.edu/master. En 2016 la revista Perspectivas Bioéticas del Programa de Bioética de la Facultad Latinoamericana de Ciencias Sociales (FLACSO) se ha incorporado a la Revista de Bioética y Derecho.

* Yasmina Soto. Licenciada en Humanidades, Universitat Autònoma de Barcelona. Máster en Bioética y Derecho, Máster (c) en Gestión de Contenidos Digitales, Universidad de Barcelona. Investigadora del Observatorio de Bioética y Derecho (OBD) de la Universidad de Barcelona. España. E-mail: yasminasoto@ub.edu.
* Trabajo presentado en la sesión especial de la Red Iberoamericana de la International Association of Bioethics (IAB) celebrada en el XIII Congreso Mundial de Bioética de la IAB: "Individuos, intereses públicos y bienes públicos", en Edimburgo (Escocia), del 14 al 17 de junio de 2016.

Resumen

La expresión *Big Data* hace referencia al tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones. Los usuarios de herramientas digitales ceden sus datos para fines concretos, por ejemplo: en las redes sociales a cambio de comunicación, en los comercios para obtener promociones y ofertas, o en las aplicaciones de salud para conseguir una relación médico-paciente más directa.

El usuario desconoce los usos posteriores: empresas externas compran o alquilan los datos cedidos para finalidades que no han sido autorizadas. Derechos del usuario como privacidad, confidencialidad y autonomía quedan vulnerados.

Los datos manejados de forma responsable son una herramienta útil para facilitar actos cotidianos, pero, empleados equivocadamente pueden convertirse en una fuente de discriminación y coacción de la autonomía.

Palabras clave: datos masivos; privacidad; ética; confidencialidad; autonomía.

Abstract

The term *Big Data* refers to the treatment of large volumes of data using mathematical algorithms in order to establish correlations between them, predict trends and to make decisions. Information and data are transferred by the users of digital tools for specific purposes, e.g.: exchange for communication in social networks, to benefit from promotions and deals in stores, or for a more direct physician-patient relationship while using Health Apps.

The user does not know potential subsequent uses of these data: external companies may buy or rent these data for purposes that have not been authorized. User rights such as privacy, confidentiality and autonomy are infringed.

Handled responsibly, these data are a useful tool to facilitate day-to-day acts, but mistakenly employed, can become a source of discrimination and coercion of autonomy.

Keywords: Big Data; privacy; ethics; confidentiality; autonomy.

1. Introducción

La traducción literal de la expresión *Big Data* es "Datos Masivos" o "datos a gran escala". Aun cuando no existe unanimidad en la definición de *Big Data*, en este trabajo se ha optado por utilizar la que emplea el Observatorio de Bioética y Derecho de la Universidad de Barcelona: "*Big Data es un término que designa el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones".*[1] Cada día se generan 2,5 quintillones de bytes de datos, y si bien no es fácil imaginar lo que supone esa gran cantidad de datos, Mayer-Schönberger y Cukier[2] proporcionan ejemplos que resultan muy visuales: "Si estuvieran impresos en libros, cubrirían la superficie entera de Estados Unidos, formando cincuenta y dos capas y si esta inmensa cantidad de datos estuvieran grabados en CD-ROMs apilados, tocarían la Luna formando cinco pilas separadas".

En el ámbito de la informática se acostumbra a hablar de datos masivos cuando cumplen el "Modelo de las tres V" (V^3):[3] Volumen, Velocidad y Variedad. El volumen, que es la principal característica del *Big Data*, hace referencia a la masiva cantidad de datos que se producen, se manejan y se almacenan. La velocidad tiene que ver con la rapidez con la que los datos se generan y circulan en la web. La variedad, que junto a la complejidad de los datos y fuentes, puede llevar a la vulneración de determinadas normativas de seguridad y privacidad de datos. Tal como refiere Joyanes (2014), se debe tener en cuenta que los riesgos por no adoptar las garantías suficientes para el manejo de datos que requiere el *Big Data* son grandes, ya que la gran cantidad de información recopilada puede llevar a una confusión que impida ver las oportunidades y amenazas.

Pese a que los conceptos de "revolución en la información" y "era digital" existen desde la década de 1960, apenas acaban de convertirse en realidad. Mucho antes del advenimiento de Internet, ya había empresas especializadas, como Equifax o Experian, que recopilaban, tabulaban y ofrecían acceso a la información personal de cientos de millones de personas de todo el mundo.

---

[1] Observatorio de Bioética y Derecho, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.

[2] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. VIII, pp. 187-211.

[3] Joyanes, L. *Big Data. Análisis de grandes volúmenes de datos en organizaciones.* Marcombo, Madrid, 2014. Cap. I. ¿Qué es Big Data? Pp. 1-44.

Entonces se sabía claramente qué información personal era identificable —nombres, números de afiliación a la seguridad social, registros fiscales, etcétera— y, como se era consciente de esta realidad, no era difícil custodiarla. Los datos recopilados se volcaban en tablas. Pero hacia los años '70, Edgar Frank Codd, especialista de IBM, propuso un nuevo instrumento para volcar, registrar y analizar los datos: las bases de datos relacionales, que permiten establecer relaciones entre los datos. Un cambio de paradigma que no ha dejado de evolucionar hasta hoy día, la fluidez de datos a través de la red y la facilidad de almacenamiento han simplificado esta tarea. Los algoritmos que se utilizan actualmente son capaces de encontrar patrones comunes en los datos con la finalidad de obtener la información que se desea y a ser posible, que puedan procesarse de forma rápida en tiempo real. En consecuencia, se debe considerar la relación entre datos en vez de la relación entre sus causas y efectos.[4]

Convertir a un individuo en una diana de vigilancia implica hoy día una invasión mucho más extensa de la vida privada, puesto que no solo se suele pretender obtener toda la información posible sobre la persona, sino también, sobre sus relaciones, conexiones e incluso, interacciones. Todo ello supone claramente una amenaza a la privacidad, pero, además, el uso de los datos masivos como modelo predictivo permite la posibilidad de poder juzgar previamente a las personas más allá de su comportamiento.[5]

La capacidad actual para almacenar y procesar datos sitúa a la mayoría de la población frente a enormes riesgos volviendo ineficaces los principales mecanismos técnicos y legales que existen actualmente para proteger la privacidad. *"Habrá menos intimidad, menos respeto a la vida privada, pero más seguridad"*, dicen las autoridades. De la mano de este imperativo se instala un régimen de seguridad al que, podemos calificar de "sociedad de control". Actualmente puede decirse que toda la sociedad funciona según el principio del "panóptico", una arquitectura carcelaria ideada por Jeremy Bentham en la cual la estructura permitía al guardián, ubicado en una torre central, observar a todos los prisioneros que estaban encerrados en celdas, sin que estos supiesen que estaban siendo observados. Los detenidos, expuestos a la oculta supervisión de los "vigilantes", viven con el temor de ser sorprendidos realizando alguna acción que estos consideren indebida, lo cual les lleva a autodisciplinarse.[6] Es interesante resaltar la deducción de Ramonet sobre que "el principio organizador de una sociedad disciplinaria es el siguiente: bajo la presión

[4] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. II, pp. 33-47.

[5] *Op. cit.* Cap. IX, pp. 211-227.

[6] Ramonet, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX nº 224, febrero 2016.

de una vigilancia ininterrumpida, la gente acaba por modificar su comportamiento".[7] Sin embargo, las sociedades de control contemporáneas dejan aparente libertad a todos los ciudadanos aunque los mantiene bajo vigilancia electrónica permanente. A veces, esta vigilancia constante y no impuesta, se lleva a cabo con sensores tecnológicos que la gente adquiere libre y voluntariamente: ordenadores, tabletas, teléfonos móviles, abonos de transporte, tarjetas bancarias inteligentes, tarjetas comerciales de fidelidad, localizadores GPS, etc".[8] Los ciudadanos facilitan datos sin tener en cuenta qué usos se pueden hacer de ellos. Por ejemplo, "*Google*, cuyo número de usuarios sobrepasa los mil millones, dispone de un impresionante número de sensores para espiar el comportamiento de cada usuario: el motor *Google Search* le permite saber dónde se encuentra el internauta, qué busca y en qué momento. El navegador *Google Chrome* envía directamente a *Alphabet*, la empresa matriz de *Google*, todo lo que hace el usuario en materia de navegación. *Google Analytics* elabora estadísticas muy precisas de las consultas de los internautas en la Red. Google Plus recoge información complementaria y la cruza. Gmail analiza la correspondencia intercambiada, lo cual dice mucho sobre el emisor y sus contactos. El servicio DNS (Domain Name System) de *Google* analiza los sitios visitados; *YouTube*, el servicio de vídeos más visitado del mundo que pertenece también a Google, y por tanto también a *Alphabet*, registra todo lo que los usuarios hacen en él. *Google Maps* identifica el lugar en el que se encuentra el internauta, adónde va, cuándo y con qué itinerario. Pero aún hay más: *AdWords* sabe lo que el empresario quiere vender o promocionar. Y desde el momento en que la gente enciende un *Smartphone* con *Android, Google* sabe inmediatamente dónde está el usuario y qué está haciendo. Obviamente nadie obliga a recurrir a *Google,* pero cuando se requiere, Google lo sabe todo sobre los usuarios".[9]

Con cada clic que hacemos, con cada desbloqueo de nuestro *Smartphone,* con cada pago a través de la tarjeta de crédito, y con las búsquedas que realizamos a través de la navegación por internet, suministramos magníficas informaciones sobre cada uno de nosotros. Datos de gran interés que, con mucha rapidez, serán analizados por corporaciones comerciales, empresas publicitarias, entidades financieras incluso por autoridades gubernamentales.[10] Obviamente se están empezando a crear economías en torno a los datos con lo que nuevos factores van a obtener beneficios de ello.

---

[7] *Op. cit.*

[8] Ramonet, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX nº 224, febrero 2016.

[9] *Google et le comportament de l'utilisateur.* Blog AxeNet. Disponible en: www.blog-axe-net-fr/google-analyse-comportement-internaute.

[10] Ramonet, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX nº 224, febrero 2016.

2. Problema

Vivimos en esta nueva era de *datificación* y *monetización* en la que la extracción de nuevos valores de los datos para rentabilizarlos tiene interés para múltiples sectores, tanto público como privado, o bien; una combinación de ambos.[11] Veamos algún ejemplo; en el ámbito privado, según Mayer-Schönberger y Cukier[12], "MasterCard tiene una división llamada MasterCard Advisors que agrega y analiza 65.000 millones de transacciones de 1.500 millones de titulares de tarjetas en doscientos diez países con la finalidad de definir tendencias de negocio y consumo. Luego vende esa información a otros. Entre otras cosas, descubrió que cuando la gente llena de gasolina el depósito del coche alrededor de las cuatro de la tarde, existe la probabilidad de que, a lo largo de la hora siguiente, gasten de treinta y cinco a cincuenta dólares en una tienda de comestibles o en un restaurante. Un publicista podría hacer uso de esa información para imprimir cupones de oferta de los negocios vecinos al dorso de los recibos de la gasolinera alrededor de esa hora del día. Como empresa intermediaria de los flujos de información, MasterCard se halla en una posición privilegiada para recopilar datos y capturar su valor. Se puede imaginar un futuro en el que las entidades emisoras de tarjetas de crédito renuncien a sus comisiones sobre las transacciones y las procesen gratuitamente a cambio de acceder a más datos, y perciban ingresos de la venta de analíticas cada vez más sofisticadas basadas en estos mismos datos".

Lo esencial del valor de los datos es su potencial de reutilización aparentemente ilimitado. Recopilar la información resulta crucial, pero no es suficiente, ya que la mayor parte del valor de los datos se halla en su uso, no en su mera posesión. Es muy difícil que una compañía sea capaz de descubrir el valor potencial de todos los datos; es por ello que, de manera más ambiciosa, muchas empresas a las que los usuarios facilitan los datos "en primicia", los licencian, firmando un acuerdo que les suponga un porcentaje del valor extraído de los mismos.[13]

Otro ejemplo, en este caso respecto al sector público: existe el proyecto PADRIS[14], que, según la Agència de Qualitat i Avaluació Sanitària de Catalunya (AQUAS) de la Generalitat de Catalunya, es un programa público de analítica de datos para la investigación y la innovación en

---

[11] Observatorio de Bioética y Derecho, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.

[12] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. VI, pp. 155-186.

[13] *Op. cit.*Cap. VI, pp. 125-153.

[14] Véase: http://aquas.gencat.cat/es/projectes/analitica_dades/.

salud. PADRIS tiene la misión de poner a disposición de la comunidad científica los datos sanitarios relacionados para impulsar la investigación, la innovación y la evaluación en salud mediante el acceso a la reutilización y cruce de los datos sanitarios generados por el sistema sanitario integral de utilización pública de Cataluña (SISCAT), de acuerdo con el marco legal y normativo, los principios éticos y de transparencia del Programa hacia la ciudadanía. Un proyecto que debe sustituir al polémico VISC+, también impulsado por la AQUAS, cuyo objetivo principal es poner la información sanitaria a disposición de los ciudadanos, empresas e investigación. Su finalidad[15] es la de mejorar "los servicios de salud y poner en valor el conocimiento" tal como indica el Observatorio de Bioética y Derecho en su documento sobre Bioética y *Big Data.*[16]

Éste proyecto se alimenta de distintas bases de datos sanitarios como por ejemplo el SIDIAP (Sistema de Información para el Desarrollo de la Investigación en la Atención Primaria) o la HC3 (Historia Clínica Compartida de Cataluña). Estas bases de datos contienen información de los usuarios de los cuales el Departament de Salut de la Generalitat de Catalunya es responsable.[17] ¿Estos datos se pondrían a disposición de terceros? Efectivamente, se considera que uno de los objetivos principales del proyecto VISC+, es poner a disposición de terceras partes la gran cantidad de datos almacenados sobre la salud de la ciudadanía catalana para que éstos puedan ser reutilizados para unas finalidades que en un inicio no estaban previstas y en consecuencia, el usuario desconoce.

Este proyecto de la Generalitat, especifica que, por un lado pretende poner los datos recopilados a disposición de centros de investigación y docencia que lo soliciten, pero por otro lado, explicita que esos datos masivos sanitarios recopilados también estarían a disposición de terceras partes. Empresas que, probablemente, utilizarían los datos para venderlos y obtener un beneficio propio, simplemente deben disponer de los medios para hacerlo y tener interés en rentabilizar la información. Con el paso de los años se opta por más flujos de información y por proteger a la población de sus excesos, no por medio de la censura, sino a través de normas que limiten el mal uso. Esto es lo que sucede con el *Big Data*, por lo que actualmente ya se están

[15] Hace referencia al Proyecto VISC+.

[16] Observatorio de Bioética y Derecho, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.

[17] *Op. cit.*

transformando muchos aspectos de la vida cotidiana y de la forma de pensar forzando a reconsiderar algunos principios básicos acerca de su crecimiento y su potencial daño.[18]

Hasta ahora, la anonimización de los datos se había considerado la garantía para cumplir con las regulaciones existentes sobre la protección de datos personales. Se parte de la base que si un conjunto de datos personales son anonimizados, éstos dejan de contener datos de carácter personal y pierden, así, el amparo de la normativa de protección de datos personales. Una normativa que pretende ser implacable tanto en la Unión Europea como en España, pero que con la vertiginosa evolución tecnológica, en un breve transcurso de tiempo, ha acaecido obsoleta.[19]

Cualquier empresa, no solo las aplicaciones para móviles o tabletas, desea obtener más información acerca de sus usuarios. Es por este motivo que se recopilan y almacenan datos y, posteriormente, se analizan. Algunas compañías, muchas de ellas anidadas en grandes corporaciones, se dedican en exclusividad a la compraventa o al alquiler de datos con una única finalidad: *conocer mejor a los usuarios para ofrecer productos que se adecúen a sus necesidades.*[20]

Una tercera parte de todas las ventas de Amazon, por lo que se dice, son resultado de sus sistemas de recomendación y personalización, utiliza los datos de sus clientes para ofrecer un producto que se adecue a sus clientes. Con estos sistemas, Amazon ha dejado fuera del negocio a numerosos competidores: no solo a muchas grandes librerías y tiendas de música, sino también a los libreros locales que pensaron que su toque personal los aislaría de los vientos de cambio. Siguiendo el ejemplo de Amazon, miles de páginas web son capaces de recomendar productos, contenidos, amigos y grupos, sin saber por qué es probable que le interesen a la gente. Todo ello vulnera derechos fundamentales como la privacidad y la intimidad.

Por ejemplo, según Caballero, "Inditex, el gigante español del sector textil, tiene su propio centro de datos en A Coruña. Emplean técnicas de *Big Data* y gracias a la gestión eficiente de los datos, cuando un cliente no encuentra una talla de una prenda, Inditex garantiza que repondrá el producto en menos de 48 horas. Para hacerlo, el sistema informático primero mira si la prenda existe en el *stock* de una tienda o centro de distribución cercano, y en caso de que no sea así, es el propio sistema informático el que solicita la fabricación de nuevas prendas. Pero no todo es

---

[18] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. IX, pp. 211-227.

[19] Observatorio de Bioética y Derecho, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.

[20] Caballero. R; Martín. E. *Las bases de Big Data.* Catarata, Madrid 2015.

gestión del *stock.* Inditex también aplica técnicas de minería de datos para averiguar qué prendas son compradas a la vez de forma habitual".[21]

Puede que los diseñadores del equipo de Inditex piensen que este otoño se lleve la combinación de prendas verdes y grises, pero al poco de lanzar la nueva línea de otoño descubran, al analizar los datos recopilados de forma inmediata de su alrededor de 7.000 tiendas en todo el mundo, que una cantidad significativa de clientes prefiere combinar el verde y el morado. Un análisis de este tipo puede llevar a cambiar la gama de colores sobre la marcha, aprovechando que las tiendas ofrecen nuevas prendas hasta dos veces por semana. Pero la utilización de los datos de ventas no acaba aquí. Este uso sería el que se consideraría autorizado por los usuarios, pero a los datos de ventas recopilados por las tiendas hay que añadir la información que se extrae sobre la navegación en las páginas de Internet de la empresa, la recopilada de forma automática por programas que examinan constantemente las redes sociales, etc. Es decir, pueden no ser los autores del acopio original, pero son los que controlan el acceso a la información y la usan directamente o la licencian para que otros extraigan su valor.[22]

3. Privacidad y confidencialidad

Se observa a través de algunos de estos ejemplos que los datos se han convertido en elementos o dispositivos de control en una sociedad cada vez más informatizada y debemos ser conscientes de por qué y para qué deben protegerse. La privacidad y la confidencialidad, en la mayoría de los casos en los que se facilitan datos, quedan vulnerada ya que otros, terceras partes, tienen acceso a información a la que el usuario no ha autorizado, no ha dado permiso para compartir, quedando dañada también la autonomía de las personas por falta de capacidad de decisión por parte del usuario. Se puede afirmar sin dudarlo que cualquier superficie comercial o plataforma digital, estructuran y categorizan sus productos según las necesidades de compra de los clientes.

Muchos usuarios de aplicaciones y también quienes se acercan a superficies comerciales, ceden sus datos para fines concretos: en las redes sociales a cambio de comunicación, en los comercios para obtener promociones y ofertas, o en las aplicaciones (Apps) de salud para conseguir una relación médico-paciente más directa. Los datos pueden ofrecer un sinfín de servicios y mejoras en el día a día, pero, muchas veces, a cambio de esas facilidades algunos de nuestros derechos son vulnerados. Las redes sociales "graban" todo lo que los usuarios "postean"

---

[21] *Op. cit.*

[22] Caballero. R; Martín. E. *Las bases de Big Data.* Catarata, Madrid 2015.

en sus perfiles, sus contactos, los "me gustas", comentarios, etc., y por lo tanto, Facebook, Twitter, Instagram, entre otras plataformas de medios sociales, lo conocen todo acerca de nuestras conexiones, opiniones y preferencias personales. De esta manera, los patrones de nuestra vida diaria se han unido al conjunto de datos personales que están disponible acerca de nosotros. Y, consecuentemente, pueden vender esta información a empresas publicitarias que, gracias al análisis de los datos acopiados, conocerán con precisión el entorno, el estado de ánimo o los gustos de los usuarios y estarán en mejor situación para ofrecer publicidad adaptada a estos datos. Repartidos ya un poco por todas partes, los detectores de nuestros actos y gestos abundan a nuestro alrededor, desde las tecnologías de reconocimiento facial que memorizan la impronta de nuestro rostro y crean, sin que lo sepamos, bases de datos biométricas de cada ciudadano. También, cedemos los datos con la finalidad de obtener promociones en superficies comerciales, las "tarjetas de fidelidad" que generosamente ofrecen la mayoría de comercios —FNAC, El Corte Inglés, Alcampo, Eroski… — para registrar los productos "favoritos" de sus clientes, conocer sus gustos y saber dónde compra. Hasta en el ámbito de la salud el modelo tradicional de atención sanitaria está viviendo un cambio de paradigma que se concreta en el auge de las *apps* de salud, conocidas como *mHealth,* y en que los usuarios tienen un trato más directo con el "médico". Ellos introducen todos sus datos y otros los reutilizan para su propio beneficio.[23]

4. Discusión

Cada clic, cada uso del teléfono, cada utilización de la tarjeta de crédito y cada navegación en Internet suministra excelentes informaciones sobre cada uno de nosotros, que se apresurara a analizar un imperio en la sombra al servicio de corporaciones comerciales, de empresas publicitarias, de entidades financieras, de partidos políticos o de autoridades gubernamentales.[24] Lo que está claro es que están empezando a crearse economías alrededor de los datos y que muchos nuevos actores van a beneficiarse de ello. "Los datos son una plataforma", ha dicho Tim O'Reilly, editor de tecnología y voz autorizada de Silicon Valley, ya que se trata de bloques de construcción para fabricar nuevos bienes y modelos de negocio.[25]

---

[23] Ramonet, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX nº 224, febrero 2016 y Mouzo, J. *La medicina montada en una "app". Las aplicaciones móviles de salud transforman la relación médico-paciente.* El País, domingo 15 de noviembre de 2015.

[24] *Op. cit.*

[25] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. IX, pp. 211-227.

Manejados de forma responsable, los datos masivos son una herramienta útil para facilitar actos cotidianos. Veamos el caso de Oren Etzioni:[26] en 2003, Etzioni tenía que volar de Seattle a Los Ángeles, por lo que meses antes entró en internet y compró un billete, creyendo que cuanto antes reserves menos pagas. Durante el vuelo, preguntó a varios pasajeros el precio de su billete y la mayoría había pagado menos que él. Etzioni estaba decidido a encontrar la forma de que la gente pudiese saber si el precio del billete de avión que ve en Internet es un buen negocio o no. Bastaba con recopilar datos y analizarlos, algo posible pero no fácil de hacer. Etzioni creó un modelo predictivo que ofrecía a sus pasajeros simulados un ahorro estimable. Ese pequeño proyecto evolucionó hasta convertirse en una empresa *start up* de nombre Farecast. Al predecir si era probable que subiera o bajara el precio de un billete de avión, y cuánto, Farecast les atribuyó a los consumidores el poder de elegir cuándo hacer clic en el botón de "comprar". Los datos se convirtieron en una materia prima del negocio, en un factor vital, capaz de crear una nueva forma de valor económico. Pero, aunque los datos se moneticen, podemos observar que, con una reutilización inteligente, se pueden convertir en un material de innovación y base de nuevos servicios.

Pero si a los datos masivos se les da un mal uso, pueden convertirse en una fuente de represión de la autonomía y de discriminación. Tales consecuencias son especialmente graves en el ámbito de la salud.[27] Es muy complejo saber dónde acaban los datos de carácter personal que recogen las aplicaciones de salud, pues casi todas las aplicaciones analizadas en un estudio compartían datos personales con terceros.[28] Las aplicaciones móviles, tabletas y relojes inteligentes pueden ayudar a la sociedad a mantenernos en forma, a perder peso, a vigilar la diabetes e incluso pueden ser útiles en el seguimiento de un cáncer y hasta monitorizando la salud mental. La salud es un aspecto crucial en la población y, es por ello que, cuanto más cerca en la cotidianeidad, más protegidos los usuarios creen que están. No es difícil imaginar el carácter privado y sensible de los datos que se vuelcan, o que se recogen en estos programas sin preguntar.

---

[26] Orem Etzioni es uno de los principales científicos estadounidenses de la computación. Concibe el universo como una serie de problemas de datos masivos: problemas que puede resolver. Y ha estado dominándolos desde el día en que se licenció en Harvard, en 1986, siendo el primer estudiante que se graduaba en ciencias de la computación. Desde su puesto en la universidad de Washington, Etzioni impulsó una gran cantidad de compañías de datos masivos antes incluso de que se diese a conocer el término. En: Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. I, pp. 11-32.

[27] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. cap. VIII, p.189.

[28] Salas, J. *¿Dónde acaban los datos privados que recogen las "apps" de salud?* El País, Ciencia. 8 de marzo de 2016. Disponible *on line*: http://elpais.com/elpais/2016/03/07/ciencia/1457369646_082762.html.

Sin embargo, lo más habitual es que el usuario viva en la inopia: ni sabe lo que comparte, ni el desarrollador de la aplicación le informa de nada. Esta falta de información tiene causas y consecuencias. La reconocida revista médica JAMA[29], ha publicado un estudio con el que ha querido llamar la atención sobre este incipiente problema que será masivo en un futuro: "Los pacientes pueden creen por error que la información que vuelcan en una *app* es privada, sobre todo si tiene política de privacidad, pero generalmente no es así" concluyen los autores de este trabajo del Instituto Tecnológico de Illinois (IIT). Además, añaden una interesante observación: el 81% de las aplicaciones no tenían política de privacidad. El resto, las que sí la tenían, no protegían la privacidad del usuario: el 80% recopilaba sus datos personales y el 50% los compartía con terceros.[30] Se debe informar al ciudadano, más allá de los beneficios que le pueda reportar una aplicación, de la importancia de ceder sus datos personales, ya que terceros están interesados en reutilizar estos datos y hacer negocio con ellos.

Actualmente, cualquier empresa, no solo las aplicaciones de móviles o tabletas, desea obtener más información acerca de sus usuarios. Hay empresas, muchas anidadas en grandes corporaciones, que se dedican exclusivamente a la compraventa o alquiler de datos con la finalidad de conocer mejor a los usuarios o a la población para ofrecer productos que se adecuen mejor a sus necesidades. Dado que no existe una cultura ciudadana de la privacidad en materia de datos personales es necesario informar a los usuarios sobre los posteriores usos de sus datos y advertirles sobre las diversas formas de reutilización lucrativa que pudieran derivarse.

Uno de los mejores ejemplos respecto a la venta o alquiler de datos a terceros lo constituye Twitter, que, obviamente, disfruta de un inmenso flujo de datos que transitan por sus servidores, pero se dirigió a dos firmas independientes a la hora de licenciarlo a otros para su uso.[31] Twitter decidió ceder los derechos sobre sus datos a dos compañías externas.

Cada vez que descargamos una App como WhatsApp o Facebook en nuestro teléfono móvil, acostumbran a solicitarnos datos de carácter personal. Una vez realizada la descarga, para poder emplear los servicios que se ofrecen se debe aceptar las bases legales de la aplicación y, con ello, se está firmando un contrato. La preocupación por lo que hacen con nuestros datos aumenta entre la población, pero la mayoría no se molesta en leer las reglas que imponen al usuario porque

---

[29] Blenner, S *et al*. *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*. March 8: Vol 315, No. 10, 2016. Disponible *on line:* http://jama.jamanetwork.com/article.aspx?articleid=2499265.

[30] Salas, J. *¿Dónde acaban los datos privados que recogen las "apps" de salud?* El País, Ciencia. 8 de marzo de 2016. Disponible *on line:* http://elpais.com/elpais/2016/03/07/ciencia/1457369646_082762.html.

[31] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. VII, pp. 155-186.

requiere demasiado tiempo y esfuerzo.[32] Mientras, las compañías de Internet se nutren de nuestros datos además de facilitárselos, en muchos casos a terceras empresas.

La complejidad que presentan los términos y condiciones de privacidad de cualquier aplicación o plataforma digital es un hecho. Las empresas que están detrás de los servicios que ofrece la era digital hilan muy fino los textos donde explican sus términos y condiciones de privacidad, entre otras especificaciones legales que afectan al usuario. Recurren a un complejo vocabulario, esconden cambios e incluyen cláusulas con algún tipo de argucia.[33]

Los usuarios de herramientas digitales, aceptan los términos y condiciones de privacidad con gran facilidad y normalmente no se detienen en una lectura de los mismos, simplemente se utiliza el *scroll* para llegar lo antes posible a la casilla de "acepto" y poder así disfrutar de los servicios que ofrecen.

5. Conclusiones

Cuando se hace referencia a la privacidad, se refiere a que la misma queda vulnerada en materia de datos personales, ya que estos se han convertido en elementos o dispositivos de control en una sociedad informatizada y es preciso ser conscientes de por qué y para qué deben protegerse. La confidencialidad se ve vulnerada ya que otros, terceros, tienen acceso a una información que el usuario no ha autorizado compartir con ellos y la autonomía resulta vulnerada por la falta de capacidad de decisión por parte del usuario, es decir que en cualquier superficie comercial o plataforma digital, estructuran y categorizan sus productos según las necesidades de compra de los clientes. Así pues, los datos personales que se registran en una cuenta se utilizan para que la empresa en cuestión obtenga unos beneficios económicos que no retornan al usuario, a pesar de que muchos consideren que el precio que pagan por el hecho de tener en su bandeja de entrada publicidad sobre productos de su interés es demasiado elevado.

En conclusión, la verdadera revolución no estriba en las máquinas que calculan los datos, sino en los datos mismos y en cómo los usamos y usaremos en el futuro.[34]

---

[32] Caballero, L. *Terminos y condiciones web*. Yorokobu. 30 de octubre de 2015. Blog. Acceso el 3 de abril de 2016. www.yorokobu.es/terminos-y-condiciones/18/?offset=29.

[33] *Op. cit.*

[34] Mayer-Schönberger, V y Cukier, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015. Cap. VIII pp. 187-209.

Bibliografía

- BLENNER, S *et al*. *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*. March 8: Vol 315, No. 10, 2016. Disponible *on line:* http://jama.jamanetwork.com/article.aspx?articleid=2499265.
- CABALLERO, R.; Martín. E*. Las bases de Big Data.* Catarata, Madrid 2015.
- CASTILLO, C. *Big Crisis Data. Social Media in Disasters and Time-Critical Situations*, Cambridge University Press, New York, 2016.
- FERNÁNDEZ, A. y GARCÍA, A. *Lliures o vassalls? El dilema digital.* El viejo Topo, Barcelona, 2017.
- MATÉ JIMENEZ, C. *Big Data. Un nuevo paradigma de análisis de datos.* Anales de mecánica y electricidad, Vol.91, Fasc, 6, 2014, pp. 10-16.
- MAYER-SCHÖNBERGER, V y CUKIER, K. *Big Data. La revolución de los datos masivos.* Turnen Noema, Madrid, 2015.
- OBSERVATORIO DE BIOÉTICA Y DERECHO, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf.
- QUINTANA GONZÁLEZ, PV. *Protección de datos, La gestión de datos personales en la PRL y la aplicación de la LOPD*. Lefebvre-El derecho, 13 de abril de 2016. Disponible en: http://tecnologia.elderecho.com/tecnologia/privacidad/gestion-datos-personales-trabajador-PRL-LOPD_11_940555001.html.
- RAMONET, I. *Google lo sabe todo de ti.* LE MONDE Diplomatique, año XX nº 224, febrero 2016.
- RAMONET, I. *El imperio de la vigilancia.* Clave Intelectual, 2016.
- SALAS, J. *¿Dónde acaban los datos privados que recogen las "apps" de salud?* El País, Ciencia. 8 de marzo de 2016. Disponible *on line*: http://elpais.com/elpais/2016/03/07/ciencia/1457369646_082762.html.
- SCHMARZO, B. *Big Data. El poder de los datos.* Anaya multimedia, Madrid, 2014.
- SWEENEY, L. *Simple demographics often identify people uniquely.* Carnegie Mellon Univesrity, editor. Data Privacy Working Paper 3, 2000. Disponible *on line*: http://dataprivacylab.org/projects/identifiability/paper1.pdf.

Fecha de recepción: 10 de octubre de 2016
Fecha de aceptación: 1 de febrero de 2017