La protección de datos personales en la red. ¿Qué ocurre con nuestros datos personales?

Laura Bernal Rodríguez

NIUB: 20193095

Curso 2019-2020

Aspectes Legals de la Informació

Abstract

El tema que ocupa este trabajo es cómo los datos personales se han convertido en la nueva moneda de cambio de los servicios digitales y el negocio que se ha creado detrás de ello gracias a la tecnología del big data. También veremos cómo han aparecido nuevas empresas que se dedican a vender los datos personales con el fin de crear perfiles de la población. Uno de los aspectos que veremos será cómo nos protege la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales junto con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para finalizar se ha analizado una sentencia con el fin de ver cómo se aplica a un caso real la legislación.

The issue of this work is how personal data have become the new currency of digital services and the business that has been created behind thanks to the technology of big data. We will also see how new companies have appeared that are dedicated to selling personal data in order to create profiles of the population. One of the aspects that we will see will be how the Organic Law 3/2018, of December 5, on the Protection of personal data and guarantee of digital rights, protects us together with Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of these data. Finally, a judgment has been analyzed in order to see how the legislation is applied to a real case.

Title: Protection of personal data on the network.

Palabras clave: protección de datos, big data, datos personales, privacidad
Keywords: data protection, big data, personal data, privacy

Tabla de contenido

Laura Bernal Rodríguez
Aspectes Legals de la Informació
2 de junio de 2020
La protección de datos en la red. ¿Estamos realmente protegidos?

1. Introducción

Los años 90 marcaron un punto de inflexión en la historia de Internet, Tim Berners-Lee creó la World Wide Web y a partir de ahí fue evolucionando hasta lo que hoy conocemos como Internet. Durante los primeros años Internet estaba formado por pocas páginas web, a mediados de la década de los 90 se inauguraron las primeras tiendas en línea, como Amazon e eBay. A partir de aquí las tecnologías han seguido evolucionando hasta la actualidad, donde podemos encender las luces de casa con comandos de voz o desbloquear nuestro teléfono inteligente con nuestra huella dactilar. Es obvio que todos estos avances tecnológicos nos facilitan la vida, pero ¿sabemos qué es lo que ocurre con todos los datos que recogen las empresas que están detrás de los dispositivos electrónicos que tenemos en casa?

Primeramente, deberíamos saber qué es lo que se consideran datos personales. Según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos),[1] los datos personales son:

> "*Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*".

Es decir, es toda esa información con la que podemos identificar a una persona. Una vez sabemos qué son los datos personales debemos saber qué derechos tenemos y qué ley es la que los ampara. En España la protección de los datos de carácter personal es una ley orgánica, es decir, es un derecho fundamental y como tal consta en la Constitución Española[2]. La ley que ampara los derechos de los ciudadanos españoles es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales,[3] «BOE» núm. 294, de 6 de diciembre de 2018, la cual nos garantiza "*los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*". El artículo 18.4 de la Constitución Española establece que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

---

1 DOUE-L-2018-80845. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) «DOUE» núm. 127, 2018. Disponible en: https://boe.gob.es/buscar/doc.php?id=DOUE-L-2018-80845.

2 BOE-A-1978-31229. Constitución Española «BOE» núm. 311, 1978. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con.

3 BOE-A-2018-16673. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales «BOE» núm. 294, 2018. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3.

Dentro de la Ley Orgánica de protección de datos 3/2018 tenemos los conocidos derechos ARCO, derecho de acceso (art. 13), derecho de rectificación (art. 14), derecho de supresión (art. 15) y derecho de oposición (art. 18), los cuales el titular de los datos puede ejercer. El derecho de acceso permite pedir al responsable del tratamiento si tus datos personales están siendo tratados o no, y si lo están siendo obtener información como por ejemplo, los fines del tratamiento, una copia de los datos personales que están siendo tratados, entre otros. Con el derecho de rectificación podemos obtener que nuestros datos personales sean rectificados si son inexactos. El derecho de supresión permite suprimir tus datos personales cuando ocurren unas circunstancias concretas, como por ejemplo: si los datos ya no son necesarios para el fin con el que se recogieron, si los datos han sido tratados ilícitamente, entre otras. Por último, el derecho de oposición permite oponerse a que el responsable realice un tratamiento de los datos personales en dos supuestos: si son objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluyendo la elaboración de perfiles; y si la finalidad del tratamiento es la mercadotecnia directa, incluyendo también la elaboración de perfiles.

2. El nuevo negocio, los datos personales

A causa de las nuevas tecnologías y de los nuevos hábitos de las personas, las empresas han tenido que reinventarse y actualizar el cómo se hacen las cosas. Una de las características que más se repiten para poder acceder a contenidos digitales es el hecho de dar tus datos personales; lo más común es que te pidan tu nombre y tu correo electrónico, pero también hay páginas web donde te piden incluso el número de teléfono. Normalmente estos sitios web nos ofrecen los contenidos de manera gratuita, pero entonces ¿por qué nos piden los datos personales para poder acceder a ellos? Esto nos hace pensar, o debería, que los datos personales que nos piden tienen algún tipo de valor, porque no suele ser habitual que se ofrezca un contenido que lleva un gran trabajo detrás de manera gratuita sin obtener nada a cambio.

Como dicen (Pacheco y Coronado, 2017, p. 1) se está desarrollando un nuevo negocio en el que los usuarios reciben servicios y contenidos digitales a cambio de que esas empresas obtengan sus datos personales, y que grandes empresas tecnológicas utilicen esos datos recogidos para que empresas como Google, Facebook, Amazon o Microsoft los exploten. El "efecto de red de datos" es lo que surge de ello, es decir, se atraen a más usuarios al usar los datos y así se generan más datos y se mejoran los servicios, lo que hace que se capten a más usuarios.

Pero ¿qué se consideran contenidos digitales? Según la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales[4], en el artículo 2.1 definen que los contenidos digitales son todos aquellos datos que han sido producidos y suministrados en formato digital, es decir, vídeo, audio, aplicaciones, juegos digitales y otro tipo de software. Por lo tanto, podríamos decir que todo lo que podemos encontrar en Internet se considera contenido digital, ya que la

[4] DOUE-L-2019-80854. Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales «DOUE» núm. 136, 2019. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80854.

gran mayoría de datos que encontramos han sido o producidos o suministrados en formatos digital.

Es importante destacar cuando se aplica esta Directiva:

> "*La presente Directiva se aplicará a todo contrato en virtud del cual el empresario suministra o se compromete a suministrar contenidos o servicios digitales al consumidor y este paga o se compromete a pagar un precio.*
>
> *La presente Directiva también se aplicará cuando el empresario suministre o se comprometa a suministrar contenidos o servicios digitales al consumidor y este facilite o se comprometa a facilitar datos personales al empresario, salvo cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales con arreglo a la presente Directiva o para permitir que el empresario cumpla los requisitos legales a los que está sujeto, y el empresario no trate esos datos para ningún otro fin."*

Lo que nos quiere decir es que la Directiva se aplicará en dos supuestos. El primero es cuando el empresario que ofrece los contenidos o servicios digitales al consumidor recibe una compensación monetaria. Y el segundo es cuando el empresario a cambio de los contenidos o servicios digitales recibe los datos personales del consumidor. Pero hay que tener en cuenta el tratamiento que hace el empresario con ellos; si esos datos personales son necesarios para llevar a cabo el suministro de los contenidos o servicios digitales, o si son necesarios para que el empresario cumpla los requisitos legales a los que está sujeto y que estos no reciban ningún tratamiento para otro fin.

Un aspecto muy importante a tener en cuenta también en cuanto a la legislación, tal y como comentan en (Martínez y Sancho, 2019, p. 13), es el hecho de la transparencia en los contratos. Es decir, el usuario debe estar informado de que la cesión de sus datos personales son la moneda de cambio por los servicios que recibe y solo si da su consentimiento[5] esos datos podrán recibir un tratamiento, tal y como se contempla en el artículo 6.1.a) del Reg. UE 2016/67: el tratamiento de los datos solo será lícito si el interesado ha dado su consentimiento para el tratamiento para uno o varios fines específicos. Relacionado a este artículo está el artículo 9.2.a) en el que explica que no queda prohibido el tratamiento de datos personales de categorías personales (como el origen étnico o racial, las opiniones políticas, entre otros y también los datos genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física) si el interesado ha dado su consentimiento explícito para el tratamiento de esos datos personales con uno o más de los fines especificados. Con estos dos artículos del Reg. UE 2016/679 podemos apreciar la importancia de que los individuos den su consentimiento para poder llevar a cabo un tratamiento de sus datos personales, de otra manera la empresa estará realizando un tratamiento ilícito.

[5] Según el artículo 4.11 del Reg. UE 2016/679 se define "consentimiento del interesado" como: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Por último, me gustaría comentar que en la consideración 58 del Reg. UE 2016/679 se expone que: "*El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice*". Lo que quiere decir esta consideración es que el usuario debe tener accesible, con un lenguaje sencillo y fácil de entender toda la información que se dirija a él; esto es necesario para que el usuario tenga conocimiento en todo momento, en el caso que nos ocupa, lo que se va a hacer con sus datos personales.

2.1 *Big data* y *data brokers*, ¿cómo afectan a nuestros datos personales?

Con la evolución de la tecnología y el aumento en la cantidad de datos que se manejan, sobre todo con YouTube, Facebook y otros servicios online alrededor de 2005, aparece el concepto de *big data*, aunque es en las décadas de 1960 y 1970 es cuando se originan los grandes conjuntos de datos. El concepto de *big data* según Gartner "son activos de información de gran volumen, alta velocidad y/o gran variedad que exigen formas rentables e innovadoras de procesamiento de información que permitan una mejor comprensión, toma de decisiones y automatización de procesos". Es decir, son datos de gran volumen, variedad y velocidad que no se pueden procesar con el software convencional por su tamaño y complejidad. También nos podemos referir al *big data* con el concepto de "ciencia de los datos".

Vinculando el *big data* con el negocio de los datos personales aparece el concepto de *data brokers* que son empresas que venden a terceras empresas datos de la vida real y virtual de las personas con fines lucrativos, es decir, empresas dedicadas al comercio de datos. Tal como se ha comentado en el apartado anterior los datos personales son el nuevo negocio y en este apartado entraremos más en detalle sobre ello.

Para empezar, el *big data* permite a las empresas que se dedican a vender datos personales crear perfiles, es decir, solo con datos básicos que obtienen de las personas pueden analizar las tendencias religiosa, política, sexual, económica, de ocio, sanitaria, policial y emocional. Estos datos los consiguen mediante la instalación de aplicaciones, registros médicos y compras en comercio; según (Oficina de Seguridad del Internauta, 2020) solo con estas acciones las personas ya dan una media de 40 consentimientos de uso de datos personales al año. Los usuarios reciben servicios de alto valor a cambio de sus datos personales. Los datos analizados son información sobre la identificación, la salud, demográfica, de vivienda, financiera, etc. Algunos ejemplos de servicios que recogen datos para ofrecer un servicio pueden ser: Facebook, Instagram, Gmail, contratar una tarjeta de crédito, participar en una encuesta, visitar páginas web, entre otros. Para evitar que las empresas guarden esa información, (Pérez, 2017) explica que Álvaro Ortigosa, director del Centro Nacional de Excelencia en Ciberseguridad (CNEC) de la Universidad de Madrid, aconseja que los usuarios pidan a las páginas web que acceden y ceden sus datos que los eliminen, es decir, que ejerzan su derecho de supresión.

La política de privacidad, la cual durante el último año las empresas han tenido que modificar para cumplir los requisitos de la Ley Orgánica de protección de datos 3/2018, es donde se informa qué es lo que ocurre con nuestros datos cuando damos el consentimiento, a dónde van, quién los maneja o durante cuánto tiempo. Tal como explica (Romero, 2018) más del 85% de los

usuarios españoles las lee "algunas veces", "raramente" o "nunca" según el avance del barómetro de mayo del Centro de Investigaciones Sociológicas, pero al 76,1% le preocupa "mucho" o "bastante" la protección de los datos personales.

Para hacernos una idea de la magnitud que han alcanzado los *data brokers* (Pérez, 2017) Amnistía Internacional ha recuperado una lista en la que revela que en Europa hay al menos 50 empresas operando de *data brokers* y en Estados Unidos o Asia no es posible saber la cantidad de empresas que operan.

(Pérez, 2017) informa del precio que tienen los datos personales, en un informe de la Amnistía Internacional se revela que la empresa Exact Data ofrece los datos de 1,8 millones de musulmanes por 126.851 euros, es decir, 7 céntimos por persona. Como podemos suponer el precio de la información depende de cuan sensible o íntima sea. (Martínez y Sancho, 2019, p. 23) explican que aunque sea complicado calcular el valor exacto de nuestros datos personales, se han creado calculadoras digitales con las que se puede estimar el valor de la información personal realizando un test. Por ejemplo, la información básica (edad, sexo y ubicación) tendría un valor de 0,0005$, unos 0,00045 euros. Si vamos añadiendo información como la marca de coche, dónde vamos de vacaciones o información financiera, la cifra sube exponencialmente.

Según (Gil, 2016, p. 51-52) una de las técnicas que se usan para que no se aplique la normativa de protección de datos es la anonimización, que consiste en hacer anónimos los datos, los cuales se convierten en datos no personales y la privacidad de los usuarios queda protegida. A parte de esta técnica, existe el proceso de disociación que aunque los datos no son anónimos tiene más garantías para la privacidad que los datos personales puros; lo que hace este proceso es crear datos pseudónimos. Aunque pensemos que así los datos están protegidos con la tecnología del *big data* es posible reidentificar a los usuarios, tanto con datos pseudónimos como con los que se consideran anónimos. Por lo tanto, estas técnicas (sobre todo la de anonimizar que es la que más protegía los datos) ya no son suficientes con el *big data*.

Por último me gustaría comentar las dos fases que tiene el proceso del *big data*, (Gil, 2016, p. 56-57) nos explica que la primera fase consiste en recolectar la información sobre los individuos y aplicar algoritmos y medios automatizados con el fin de observar correlaciones, y así extraer conclusiones de la manera en la que afecta una circunstancia específica al comportamiento del individuo. Es decir, esta fase lo que busca es encontrar correlaciones entre los grupos de datos, creando un modelo con ello, y mantener la confianza de que los datos no estén contaminados. La segunda fase aplica el modelo creado a una persona determinada, es decir, los datos de la persona se procesan y junto con el modelo que se ha creado se obtienen conclusiones sobre ella. El consentimiento informado de la persona en esta fase es necesario. En esta fase el riesgo ético es mucho mayor porque se obtienen conclusiones de los individuos y su uso puede ser beneficioso, pero también puede ser discriminatorio.

3. La SAN, 1ª, 19.10.19, ¿son los datos biométricos datos personales?

A la hora de buscar sentencias en las que aparezca la Ley Orgánica de protección de datos 3/2018 es complicado por el poco tiempo que ha transcurrido desde su aprobación, por lo tanto, la

sentencia que se analizará en este apartado está resuelta con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.[6]

El 19 de septiembre de 2019 la entidad mercantil "FITNESS MURCIA PROMOTIONS S.L" interpuso un recurso frente a la resolución de la Directora de la Agencia Española de Protección de Datos, con fecha 25 de julio de 2018, donde confirma en reposición la resolución de 14 de junio de 2018. Este recurso se llevó a cabo en la Sala de lo Contencioso-Administrativo de la Audiencia Nacional; y lo que pide la parte actora es que la sanción de 1.500€ impuesta el 14 de junio de 2018 quede sin efecto.

La parte actora recibió la sanción de 1.500€ por una infracción del artículo 4.1 de la Ley Orgánica de protección de datos 15/1999, dicha infracción está tipificada como grave en el artículo 44.3.c). El artículo 4.1 de la LOPD 15/1999 nos indica que: "*Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*" y el artículo 44.3.c) indica que es una infracción grave el: "*Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible*".

La AEPD expone que la parte actora ha incurrido en dicha infracción por el tratamiento[7] que han recibido los datos de reconocimiento de huella dactilar por parte de los usuarios del gimnasio para controlar el acceso, siendo este el único modo de acceder. También expone que utiliza los datos de forma no proporcionada y excesiva en relación con el ámbito y finalidades determinadas. Además, señala que se podría conseguir el mismo objetivo de control de acceso si en vez de usar el control biométrico se usase una tarjeta inteligente que contenga el propio dato biométrico o el algoritmo del socio, por lo tanto, no se incorporarían en el sistema los datos biométricos.[8]

La razón por la que la empresa Fitness Murcia Promotions es denunciada es porque a partir del 2 de febrero de 2017 cambiaron el sistema de acceder al centro mediante el uso de la huella dactilar en vez del uso de la pulsera. A la hora de tomar la huella dactilar la empresa genera una plantilla numérica o patrón utilizando algunos puntos de la huella generados a partir de algoritmos matemáticos, es decir, a través de algunos puntos de la huella dactilar generaban un código único. El objetivo de este cambio es para evitar que se intercambien las tarjetas u otros dispositivos para identificar a los socios con otros usuarios. Los puntos de la huella recogida los

[6] BOE-A-1999-23750. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal «BOE» núm. 298, 1999. Disponible en: https://www.boe.es/eli/es/lo/1999/12/13/15/con.

[7] Según el Reglamento 2016/679 un tratamiento es: "C*ualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*".

[8] Según el Reglamento 2016/679 los datos biométricos son: "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*".

almacenan en el sistema transformados en un algoritmo matemático, el encargado de dicho tratamiento es la entidad Proyectos Visuales Zaragoza S.L. (PROVISPORT).

La parte actora sustenta su pretensión impugnatoria en dos motivos. El primer motivo es que los datos que están recogiendo no pueden ser considerados datos de carácter personal, ya que no permite la identificación de los titulares al no recoger la huella, ni almacenarla, sino una parte de esta y después transformada en un código numérico. Sin embargo, en el artículo 5.1.f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de protección de datos 15/1999, de 13 de diciembre, de protección de datos de carácter personal,[9] definen los datos de carácter personal como: "*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*", por lo tanto, según esta definición los datos biométricos sí que se consideran datos de carácter personal porque proporcionan información sobre una persona determinada. El segundo motivo es, porque el uso del sistema implantado es adecuado al artículo 4.1 de la LOPD 15/1999. Argumentan que tanto los datos de la huella como del algoritmo no están almacenados en una tarjeta y que no han sido incorporados al sistema o a la base de datos.

En el artículo 6.1 de la Ley Orgánica de protección de datos 15/1999 se especifica que: "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa*" y la empresa informa al usuario en el contrato el uso de sus datos biométricos para controlar el acceso a las instalaciones y que esta medida será la única con la que se podrá acceder.

Finalmente, retiran la sanción de 1.500€ impuesta a la empresa "FITNESS MURIA PROMOTIONS S.L", ya que con los argumentos que ha expuesto esta se ha considerado que no infringe el artículo 4.1 de la Ley Orgánica de protección de datos 15/1999.

En esta sentencia se ha hablado mucho del tratamiento de los datos de carácter personal, en este caso de las huellas dactilares, y a parte de todos los artículos que se nombran en la sentencia también podemos encontrar en el Reg. UE 2016/679 el artículo 6. Licitud del tratamiento, donde se exponen las condiciones en la que un tratamiento sería lícito siempre y cuando se cumpla mínimo una. Una de las condiciones que vemos que en este caso se cumplen es la primera, el artículo 6.1.a) dice: "*el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos*", es decir, que el socio del gimnasio da su consentimiento para el tratamiento de su huella dactilar con el fin de acceder a las instalaciones y en el contrato especificaban que esta era la nueva y única manera de acceder, por lo tanto, es un tratamiento lícito.

[9] BOE-A-2008-979. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. «BOE» núm. 17, 2008. Disponible en: https://www.boe.es/eli/es/rd/2007/12/21/1720/con.

4. Conclusiones

Antes de empezar a hacer este trabajo ya sabía en cierta medida que el poder mantener la privacidad de nuestros datos personales en Internet es algo muy importante y también bastante complicado porque cada movimiento que hacemos en la red ya estamos enviando datos sobre nuestros gustos, nuestra geolocalización, etc. Pero lo que no tenía claro es la cantidad de empresas que se dedican a la venta de estos datos personales que recogen y mucho menos el precio que éstos tienen en el mercado; me ha sorprendido que la información básica de una persona tenga un precio tan bajo.

Como consumidora de Internet siento que no estamos realmente informados de lo que se hace con nuestros datos personales y de cuánta importancia tiene el que podamos mantener nuestra privacidad en todo momento, tanto por culpa de las empresas que no suelen usar un lenguaje sencillo para que todas las personas sean capaces de entender qué tratamiento o qué uso tendrán sus datos personales, además de la longitud que tienen las políticas de privacidad. Pero también tenemos parte de culpa las personas que hacemos uso de los servicios, ya que tal y como se ha comentado en el trabajo solo un 15% se lee las políticas de privacidad que es donde las empresas están obligadas a explicar qué es lo que se va a hacer con los datos personales recogidos, y por lo tanto, es donde nos podemos informar de ello y así saber si nos interesa cambiar nuestros datos personales por sus servicios.

Como se ha podido comprobar detrás de los datos personales hay un gran negocio con el que muchas empresas, los *data brokers*, obtienen beneficio al vender la información y los perfiles que han podido crear sobre los individuos gracias al *big data*. Cada vez es más importante aprender a mantener nuestra privacidad a salvo de estas empresas, ya que cada vez con la evolución de las tecnologías y la creación de nuevas redes sociales que piden permisos de nuestro teléfono móvil (de localización, la cámara, el micrófono, etc.), tienen más facilidad para obtener nuestros datos personales.

En cuanto a la legislación, la Ley Orgánica de protección de datos 3/2018, es importante tener en cuenta que solo se aplica si la información hace que las personas físicas sean identificadas o identificables. Es decir, si con la información no se puede identificar a la persona física no se aplicaría. Esta ley protege a los usuarios de que las empresas hagan un mal uso de nuestros datos personales, pero es imprescindible ser conscientes de dónde introducimos nuestros datos personales y el tratamiento que van a recibir. Además, es importante saber que es necesario nuestro consentimiento para que nuestros datos personales puedan recibir un tratamiento sino sería ilícito, tal y como se expone en los artículos 6.1.a) y 9.2.a) del Reg. UE 2016/679.

Por último, nunca me había planteado si nuestros datos biométricos son datos personales o no, ya que es una tecnología que lleva unos pocos años implementada en nuestro día a día con los teléfonos inteligentes y personalmente no la he usado más allá de este. Pero al analizar la SAN, 1ª, 19.10.19, me he dado cuenta de que poco a poco está ganando más terreno la tecnología del desbloqueo con huella dactilar, y al ser datos que hacen que una persona física sea identificada deben estar protegidos también por la Ley Orgánica de protección de datos 3/2018.

5. Tabla de jurisprudencia citada

Audiencia Nacional

Resolución y fecha	Asunto y referencia	Magistrado Ponente	Partes
SAN, 1ª, 19.10.19	JUR\2019\288495, ECLI:ES:AN:2019:3675	Mª Luz Lourdes Sanz Calvo	Fitness Murcia Promotions S.L. v. Agencia Española de Protección de Datos

6. Bibliografía

- Elena GIL GONZÁLEZ, "Big Data. Privacidad y protección de datos", Imprenta nacional de la Agencia Estatal, Madrid, 2016, disponible en: https://www.aepd.es/sites/default/files/2019-10/big-data.pdf.
- Luz M. MARTÍNEZ VELENCOSO, Marina SANCHO LÓPEZ, "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", *InDret 1/2018*, Barcelona, 2019, disponible en: https://indret.com/wp-content/uploads/2018/03/1371.pdf.
- Mª Nieves PACHECO JIMÉNEZ, Mikael LEAL CORONADO, "Nueva moneda de cambio: Nuestros datos personales como pago de contenidos digitales", *Centro de Estudios de Consumo*, 2017,disponible en: http://centrodeestudiosdeconsumo.com/images/Contenidos_digitales_e_intercambio_datos.pdf.

Otras fuentes

- "Derecho de acceso", *Agencia Española de Protección de Datos*, 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-acceso.
- "Derecho de oposición", *Agencia Española de Protección de Datos*, 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-oposicion.
- "Derecho de rectificación", *Agencia Española de Protección de Datos*, 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-rectificacion.
- "Derecho de supresión ("al olvido")", *Agencia Española de Protección de Datos*, 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido.
- "Gartner Glossary", *Gartner*, disponible en: https://www.gartner.com/en/information-technology/glossary/big-data.
- "Los Data Brokers y su interés por nuestros datos", *Oficina de Seguridad del Internauta*, 2020, disponible en: https://www.osi.es/es/actualidad/blog/2020/01/14/los-data-brokers-y-su-interes-por-nuestros-datos.
- "Qué es big data", *Oracle*, disponible en: https://www.oracle.com/es/big-data/what-is-big-data.html.

- "Tienda en línea", *Wikipedia*, disponible en: https://es.wikipedia.org/wiki/Tienda_en_l%C3%ADnea.
- Pablo ROMERO, "El CIS confirma lo que todos sospechamos: casi nadie se lee las políticas de privacidad", *Público*, 2018, disponible en: https://www.publico.es/sociedad/proteccion-datos-cis-confirma-sospechamos-nadie-lee-politicas-privacidad.html.
- Rosario G. GÓMEZ, "El nuevo mundo tejido por la WWW", *El País*, 2019, disponible en: https://elpais.com/elpais/2019/03/17/opinion/1552844121_038494.html.
- Susana PÉREZ DE PABLOS, "Tus datos se venden por 7 céntimos de euro", *El País*, 2017, disponible en: https://elpais.com/tecnologia/2017/05/03/actualidad/1493835469_309268.html.