Universidad de La Laguna
Facultad de Derecho

Grado en: Relaciones Laborales

Facultad de Derecho

Universidad de La Laguna

Curso: 2017/2018

Convocatoria: Junio

BIG DATA Y PROTECCIÓN DE DATOS

Big data and data protection

Realizado por el alumno/a D. Itahisa María Yapci Marante Pérez

Tutorizado por la Profesora Susana Eva Franco Escobar

Departamento: Derecho Administrativo

Área de conocimiento: Derecho Administrativo

ABSTRACT

It is often heard the term "Big Data", which makes reference to a technology based on massive data analysis. These data are daily generated by ourselves using the Internet, for example. However, these data are usually personal, and therefore it is essential to keep in mind the current legislation to guarantee a correct use of this technology.

In this work it will be tackled about what Big Data is, what problems related with protection of personal data appear when it is used, what laws could be applied in these cases and, from a legal point of view, the solutions that can be took to guarantee our right to privacy. Besides, it will be made an analysis about user rights and the application of different jurisdiction, highlighting the international data transfers between Europe and the USA and the consents and permissions required to use citizens data.

Finally, even with the entry into force of the European Regulation, it is a fact that our right to privacy can be easily infringed. Therefore, as well as the current legislation must be respected, citizens should become aware of the importance of give personal data and how dangerous it could be for our right to privacy.

RESUMEN

A menudo se oye hablar del *Big Data*, término que hace referencia a la tecnología basada en el análisis masivo de datos. Datos que, por ejemplo, generamos nosotros mismos diariamente a través de internet. El problema radica en que generalmente estos datos son de carácter personal, por lo que se hace imprescindible tener en cuenta la legislación vigente para el correcto uso de esta tecnología.

A lo largo de este trabajo se planteará en qué consiste el *Big data*, qué problemas se generan al utilizarlo con respecto a la protección de datos de carácter personal, qué leyes son de aplicación en estos casos y qué soluciones existen desde el punto de vista legal para preservar nuestro derecho a la intimidad. Se hará un análisis sobre los derechos de los usuarios y la aplicación de fueros diferentes, haciendo hincapié en las transferencias internacionales de datos entre Europa y EE.UU. y los consentimientos y permisos necesarios a la hora de utilizar los datos de los ciudadanos.

Por último, aun con la entrada en vigor del Reglamento Europeo, es un hecho que nuestro derecho a la intimidad puede ser vulnerado con facilidad. Es por ello por lo que, además de respetar la legislación vigente, es necesario concienciar a la población sobre la importancia de ceder datos personales y el riesgo que supone para nuestro derecho a la intimidad.

Índice

1. INTRODUCCIÓN 5
1.1 Qué es Big data *5*
1.2 Problemas de conciliación con el derecho a la intimidad *9*
1.3 Soluciones: Reglamento europeo *10*
1.4 Problemas subsistentes *16*
1.5. En especial, en el ámbito laboral *18*
2. ANÁLISIS 19
2.1 Derecho a la intimidad, a la protección de datos y al olvido *19*
2.2 Fueros *21*
Transferencia internacional de datos con EE.UU. *25*
2.3 Consentimiento *30*
El consentimiento en las cookies. *31*
Permisos de las aplicaciones *34*
2.4 Sanciones *36*
2.5 Caso Facebook *39*
3. CONCLUSIONES 42
4. BIBLIOGRAFÍA 44

1. INTRODUCCIÓN

1.1 Qué es Big data

No existe una definición absoluta, ya que es una tecnología nueva, que aún está en desarrollo, pero al hablar de *Big data* nos referimos a una cantidad masiva de datos (estructurados y no estructurados), un aspecto importante a la hora de hablar de esta tecnología. El *Big data* se ha caracterizado también por las denominadas cuatro uves: volumen, velocidad, variedad y valor. En primer lugar, el volumen define la gran cantidad de datos, es decir, el procesamiento de un gran volumen de información no estructurada, transformándola finalmente en información útil para el usuario. En segundo lugar, la velocidad determina el ritmo con el que los datos se reciben y se realiza una acción a través de ellos mediante la información analizada. Por otra parte, la variedad hace referencia a la diversidad de datos que se analizan, es decir, los datos no se encuentran estructurados y la complejidad para analizarlos aumenta. Finalmente, el valor representa la utilidad intrínseca que se genera a posteriori con el análisis de toda esta información[1].

La privacidad se plantea como una necesidad en un mundo en el que cada vez más, todos los usuarios comparten continuamente su información personal, datos relativos a su ubicación de forma constante, datos personales en redes sociales, etc. En los sistemas actuales se debe priorizar en la necesidad de proteger los datos de modo que no se pueda acceder a la información de los usuarios y realizar acciones por terceros para obtener beneficio con sus datos.

El término de *Big data* se aplica a los conjuntos de datos de gran volumen, que provienen de diversas fuentes y la forma en la que se gestionan. El uso y análisis de estos datos permite una mejor y rápida toma de decisiones. A través de diferentes técnicas y

[1] Espinoza Paredes, S. (2015). Generar un marco de referencia para implementaciones de Big Data para telecomunicaciones, caso de estudio corporación nacional de telecomunicaciones. [online] Disponible en: http://dspace.udla.edu.ec/bitstream/33000/3419/1/UDLA-EC-TMGSTI-2015-17%28S%29.pdf [Acceso el 12 de diciembre de 2017].

metodologías como el análisis de texto, las estadísticas o el análisis predictivo se puede obtener y analizar la información para la obtención de resultados[2].

El *Big data* trata una gran cantidad de datos diferentes, los datos se recopilan de una gran variedad de fuentes y los análisis aplicados son cada vez más complejos. Cuando estos datos contienen información personal existen múltiples implicaciones para la privacidad y la protección de datos. Las empresas y los gobiernos utilizan cada vez más el *Big data* para predecir información, generar estadísticas, obtener ratios, detectar correlaciones, percibir patrones, etc. Esto genera un problema en cuanto a la privacidad y la protección si estos datos contienen información personal de los usuarios[3].

En los últimos años se ha iniciado un debate mundial acerca de las implicaciones del *Big data* y la necesidad de la protección de los datos por parte de legisladores y reguladores. Lo que ha generado que diferentes regiones a grandes niveles hayan comenzado a legislar la protección de datos. Es necesario identificar y modelar la información accesible y pública de las personas para que las técnicas utilizadas de privacidad conserven la utilidad de estos datos, cumplan las leyes de protección de datos y no exista vulnerabilidad en la privacidad de la información.

El volumen de información crece de manera tan rápida en los últimos años que se han creado nuevos términos para su medición como zettabyte o yottabyte. Según IBM[4], la producción actual de datos se encuentra en los 2,5 quintillones de bytes cada día, lo que ha producido que el 90% de los datos en el mundo se haya creado en los dos últimos años. Este número aumenta exponencialmente a medida que cada vez más se conectan más dispositivos electrónicos y se incrementa la red de nodos conectados a la red. Además de

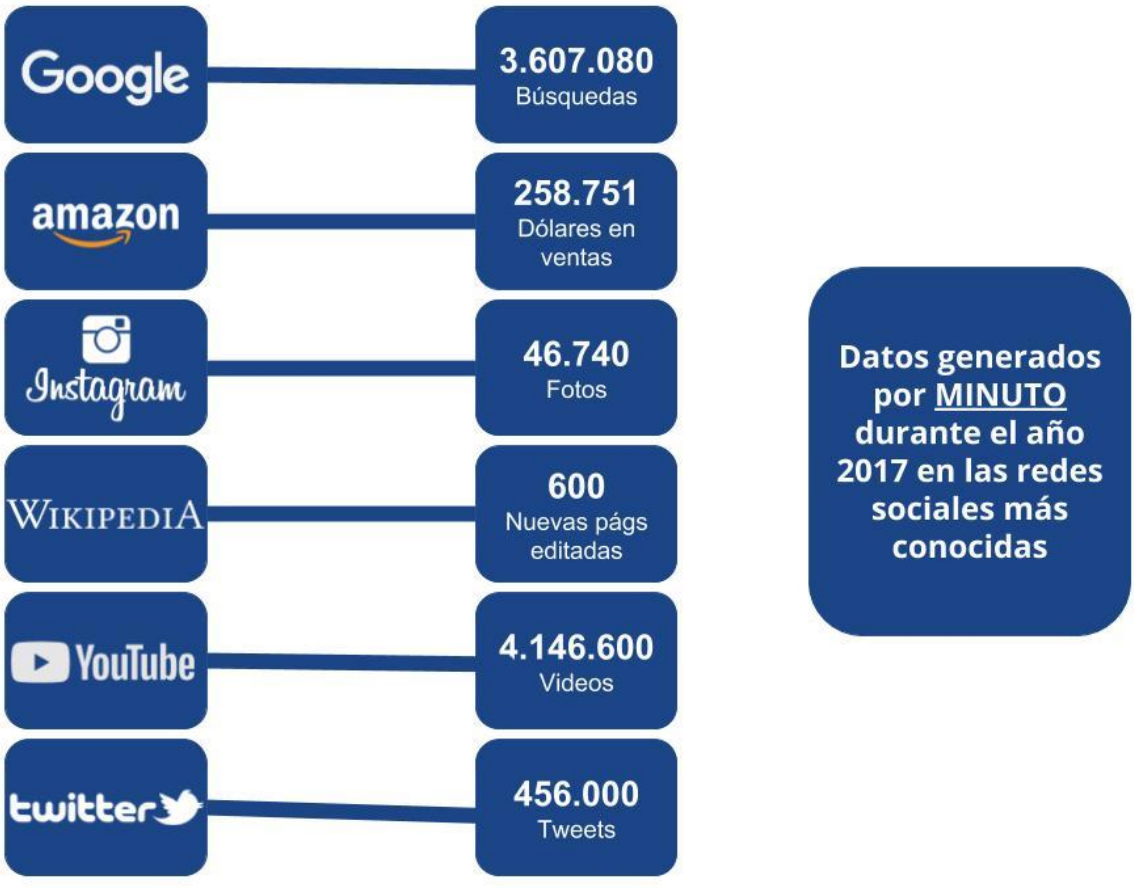
[2] Espinoza Paredes, S. (2015). Generar un marco de referencia para implementaciones de Big Data para telecomunicaciones, caso de estudio corporación nacional de telecomunicaciones. [online] Disponible en: http://dspace.udla.edu.ec/bitstream/33000/3419/1/UDLA-EC-TMGSTI-2015-17%28S%29.pdf [Acceso el 12 de diciembre de 2017].

[3] Ferrer-Sapena, A., & Sánchez-Pérez, E. (2013). Open data, big data: ¿Hacia dónde nos dirigimos? *Anuario ThinkEPI 2013*, *7*, 150-156.

[4] Www-01.ibm.com. (2018). *IBM – Big Data - Argentina*. [online] Disponible en: www-01.ibm.com/software/ar/data/bigdata/ [Acceso 17 de mayo de 2018].

esto, los datos digitales se pueden compartir, combinar o duplicar fácilmente, aumentando su tamaño, además también por los metadatos que la acompañan (cuándo, dónde y cómo se generó esta información). Hay cada vez más personas utilizando y compartiendo sus datos en Internet y de muchas maneras diferentes (redes sociales, correo electrónico, Internet de las cosas, dispositivos móviles, etc.).

En el año 2017 los usuarios que utilizan internet habitualmente han aumentado hasta los 3,7 miles de millones de personas. En el esquema siguiente se pueden apreciar datos destacados en la generación de información por minuto en Internet, como por ejemplo los 3,6 millones de búsquedas en Google.



5

[5] Domo.com. (2017). *Data Never Sleeps 5.0 | Domo*. [online] Disponible en: https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1 [Acceso 17 mayo 2018].

El tráfico de datos por la red de redes se triplicó de 2013 a 2018 pasando de 255 exabytes por mes en 2013 a 715 exabytes por mes en 2018. Por otro lado, si en 2015 eran 1,387 millones los usuarios de servicios de computación en la nube, en 2018 se alcanzaron los 2 millones: un aumento en torno al 18%[6].

El *Big data* es un instrumento útil, que contribuye por ejemplo a la toma inmediata de decisiones en las empresas, nos hace la vida más fácil a la hora de buscar información, pero por otro lado genera algunas dudas en cuanto a la privacidad de las personas, muchos se preguntan dónde está el límite en relación con la protección de datos.

Nuestras compañías telefónicas pueden saber, sólo analizando nuestros teléfonos móviles, dónde estamos en todo momento; las diferentes aplicaciones que descargamos nos piden permisos ilógicos como la ubicación o acceso a cámaras, y muchas veces no nos fijamos: estas aplicaciones son gratuitas, pero se nutren desde el punto de vista económico de nuestros datos. "Si un servicio es gratuito, el producto eres tú"[7].

Generamos a través de internet una cantidad inimaginable de datos que es imposible gestionar para los humanos, sin embargo, cada vez existen más herramientas que permiten tratar estos datos por medio de algoritmos cuyos resultados son utilizados por diferentes agentes sociales para su propio beneficio. Todos nuestros datos quedan almacenados y es necesario establecer una legislación que regule estas situaciones. Con todo esto tiene mucho que ver el derecho a la protección de datos y el derecho al olvido.

[6] CISCO, Cloud Index White Paper, 2013-2018. [online] Disponible en: www.terena.org/mail-archives/storage/pdfVVqL9tLHLH.pdf [Acceso el 12 de diciembre de 2017].

[7] Mallol, E., Plasencia, A. and S.L.U., U. (2018). 'Debes saber que si un servicio es gratuito el producto eres tú'. [online] ELMUNDO. Disponible en: http://www.elmundo.es/economia/2014/11/28/547772eee2704e295e8b457d.html [Acceso el 12 de diciembre de 2017].

1.2 Problemas de conciliación con el derecho a la intimidad

"*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*"[8]. El artículo 18.1 de la constitución española nos habla del derecho a la intimidad personal y familiar, pero ¿qué es, y cuáles son los límites de este derecho?

El derecho a la intimidad es un derecho fundamental irrenunciable, esto no implica que a través de un consentimiento expreso podamos renunciar a una parte (por ejemplo, con permisos al descargarnos una aplicación), o que las autoridades puedan autorizar, en favor del interés público, determinadas entradas en la intimidad personal.

La intimidad es un concepto complicado porque obedecerá a nuestra percepción, lo que es íntimo y lo que no lo es para cada persona, del momento y del lugar. Pero para centrarnos, la ley establece que se vulnera el derecho a la intimidad cuando se trata de grabar o reproducir la vida íntima de las personas, poner en conocimiento de otros cartas privadas, divulgación de hechos relativos a la vida privada de otras personas que afecten a su reputación y buen nombre, revelación de datos privados de personas conocidas a través de la actividad profesional de quién los revela, utilización de la voz o la imagen de una persona para fines publicitarios o comerciales, imputación de hechos o manifestación de juicios de valor a través de acciones o expresiones que lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación[9].

Pero, tenemos aceptado que no tenemos intimidad, es decir, no es posible una intimidad total, a pesar de su condición de derecho fundamental. Hay cámaras en las calles, existen empresas que utilizan nuestras redes sociales para saber cómo somos, bancos que utilizan algoritmos para decidir si conceden un préstamo o no en función de todos los datos que

[8] Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311.
[9] España. Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado, 14 de mayo de 1982.

se almacenan, nuestros datos, son utilizados en mayor o menor medida, pero muchas veces no les damos importancia al no considerarlos íntimos.

El derecho a la intimidad es subjetivo, lo que para unas personas es íntimo para otras no lo es, el *Big data* puede vulnerar el derecho a la intimidad en la medida en que utilice datos más o menos sensibles. El problema de esta nueva tecnología es que las leyes actuales españolas fueron desarrolladas antes de la gran expansión de las nuevas tecnologías, nos hablan de grabaciones de voz, de cartas, pero no tienen en cuenta la grandísima cantidad de datos que se generan a diario a través de internet.

1.3 Soluciones: Reglamento europeo

A raíz de polémicas como la de Facebook, WhatsApp o WikiLeaks la población empieza a experimentar una gran falta de confianza en internet y los datos que se generan, algo que podríamos considerar positivo si sirve para que nos fijemos en qué permisos damos a las aplicaciones, qué permitimos que se haga con nuestros datos. Los usuarios, la mayoría de las veces, no leemos las condiciones de privacidad y no nos paramos a pensar en qué permisos damos al descargar una aplicación.

Del mismo modo que la sociedad evoluciona mucho más rápido que las normas jurídicas, la tecnología avanza mucho más rápido que el derecho. No es posible crear una ley para cada innovación tecnológica, y siempre se va un paso por detrás, puesto que es imposible prever las nuevas técnicas informáticas o legislar en base a las posibilidades del futuro.

La Unión Europea ha aprobado una legislación que unifica las normas relativas a la protección de datos en todos los estados miembros. El nuevo reglamento, no requiere de normas internas de trasposición, ni de normas de desarrollo o aplicación. A partir de mayo de 2018 este nuevo reglamento será de aplicación en todos los estados miembros, se asumirá como norma de referencia ésta y no las nacionales y quedará derogada la Directiva 95/46. La ley que sustituirá a la actual Ley Orgánica de Protección de datos

podrá incluir algunas precisiones o desarrollos en las materias en las que el reglamento lo permita[10].

La regulación general de protección de datos aprobada el 14 de abril de 2016, en adelante RGPD[11], supone la unificación de legislación en todos los Estados miembros de la Unión Europea. El reglamento establece normas relativas al tratamiento de los datos personales y a la libre circulación de tales datos. Este reglamento será de aplicación en todos los Estados miembros, ello supone un salto cualitativo en la legislación y también se aplica a empresas que, a pesar de no tener su sede en países europeos, presten sus servicios dentro de la U.E., como establece el derecho internacional.

En relación con la Ley Orgánica de Protección de Datos Personales, en adelante LOPD[12], el nuevo reglamento europeo presenta una serie de novedades, siendo más restrictivo en lo que al tratamiento de datos personales se refiere. Por un lado, en el nuevo reglamento europeo aparece el principio de responsabilidad proactiva que requiere que las organizaciones analicen que datos tratan, con que finalidad y que tipo de operaciones de tratamiento llevan a cabo, las organizaciones deben poder demostrar ante los interesados y ante las autoridades que cumplen con las medidas que establece el reglamento. Por otro lado, el reglamento europeo exige, en el caso de que se trate una cantidad masiva de datos que se tenga en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento y el riesgo para los derechos y libertades de las personas.[13]

[10] Agencia Española de Protección de datos, (2018). *Guía del reglamento general de protección de datos para responsables del tratamiento*. [online] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf [Acceso el 5 de marzo de 2018].

[11] Unión Europea. 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).

[12] España. Ley Orgánica 14/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 13 de diciembre de 1999, núm 298.

[13] Agencia Española de Protección de datos, (2018). *Guía del reglamento general de protección de datos para responsables del tratamiento*. [online] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf [Acceso el 5 de marzo de 2018].

Uno de los cambios con respecto a la LOPD se encuentra en la información que recibe el ciudadano que no sólo debe ser expresa, precisa e inequívoca, sino que además será concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo para cumplir con el principio de transparencia que exige el reglamento en su artículo 12.

En el RGPD se recalca la necesidad de un consentimiento inequívoco, libre y revocable, que deberá otorgarse por medio de un acto afirmativo y claro. A partir de su entrada en vigor el silencio, las casillas ya marcadas o la inacción no darán lugar a un consentimiento válido. Es necesario que en el consentimiento aparezcan de forma clara y concisa para que serán utilizados los datos. Con el nuevo reglamento se pone de manifiesto la necesidad de la transparencia en el tratamiento de los datos, tanto en la finalidad de estos, como en los períodos que deben ser guardados[14].

En los artículos 16 y 17 del RGPD se determinan los derechos de rectificación y suspensión. El primero de ellos hace referencia a la posibilidad de que el interesado pueda cambiar los datos que le conciernen cuando estos sean incorrectos o estén incompletos. Mientras que el derecho de supresión o derecho al olvido implica que los datos que del interesado pueden ser eliminados cuando se den una serie de circunstancias, por ejemplo, el tratamiento ilícito de los datos, la desaparición de la finalidad que motivó el tratamiento o recogida, cuando se revoca el consentimiento o cuando te opones a que se traten los datos.

El derecho a la supresión o derecho al olvido se relaciona de manera directa con el principio de calidad de los datos, estos deben ser lícitos, leales y transparentes, además deberán ser recogidos con un fin explícito y legítimo, tendrán que ser adecuados a los principios de proporcionalidad, exactitud y actualización. Es importante tener en cuenta que el derecho al olvido tiene su propio ámbito de aplicación que se concreta en el control

[14] Sánchez Barroso, M. (2016). *Iniciando el camino para cumplir con la nueva Regulación Europea de Protección de Datos*. [online] SSa Asesores. Disponible en: https://ssa-asesores.es/html/wordpress/blog/2016/05/19/iniciando-el-camino-para-cumplir-con-la-nueva-regulacion-europea-de-proteccion-de-datos/ [Acceso el 5 de marzo de 2018].

efectivo sobre los datos personales en la autodeterminación informativa del propio individuo, cuyo refuerzo fija uno de los propósitos que pretende el RGPD[15].

El RGPD en el artículo 21, establece el derecho de los ciudadanos a oponerse al tratamiento de datos que le conciernen, por motivos personales, especialmente cuando el tratamiento tenga por objeto el marketing directo, salvo que el encargado acredite un interés legítimo.

La limitación al tratamiento de los datos personales supone que no se aplicarán a los datos del interesado las operaciones que en cada caso corresponderían. Este derecho reconoce la potestad de los interesados para solicitar al responsable una limitación del tratamiento de sus datos personales, los datos personales deberán reservarse y ser utilizados solo en el caso de que exista consentimiento por parte del interesado o por razones de interés público. El interesado deberá ser informado cuando se vayan a utilizar de nuevo sus datos personales y se deje de aplicar la limitación[16].

Se puede solicitar la limitación cuando el interesado ha ejercido su derecho a la rectificación u oposición. Cuando el tratamiento es ilícito, que supondría el borrado de los datos, pero el interesado se opone a ello. Cuando los datos ya no son necesarios, pero el interesado los necesita para el ejercicio o defensa de reclamaciones. Durante el tiempo que dure la limitación el responsable solo podrá tratar los datos afectados, cuando cuente con el consentimiento del interesado, para la formulación o la defensa de reclamaciones o para proteger los derechos de otra persona física o jurídica. El derecho de limitación no debe confundirse con el bloqueo de datos que establece la LOPD. Con el derecho de

[15] Berrocal Lanzarot, A. (2017). *Derecho de supresión de datos o derecho al olvido*. 1st ed. Madrid: Reus, S.A., pp. 214-215

[16] García Martín, I. (2016). *Nuevo derecho reconocido por el Reglamento Europeo de Protección de Datos; "Limitación del Tratamiento"*. [online] Picón y asociados, abogados. Disponible en: https://www.piconyasociados.es/noticias/nuevo-derecho-reconocido-por-el-reglamento-europeo-de-proteccion-de-datos-limitacion-del-tratamiento/ [Acceso el 5 de marzo de 2018].

limitación se impiden borrar los datos cuando se ejercitan otros derechos, ya que esto impediría el ejercicio del derecho a la limitación del tratamiento[17].

El derecho de portabilidad se incluye en el RGPD y consiste en que los datos pueden ser transmitidos de un fichero a otro cuando el interesado lo solicite, siempre que sea técnicamente posible. Este derecho permite a las personas obtener los datos que hayan dado a una entidad en un formato estructurado de uso común y de lectura mecánica. Con este derecho aparece la posibilidad de que los datos sean transmitidos a otro proveedor de servicios. El objetivo de esta nueva incursión es que el ciudadano pueda trasladar, copiar o trasmitir sus datos personales de un entorno informático a otro.

En relación con el responsable del tratamiento de los datos el RGPD en su capítulo IV diferencia en los distintos títulos las obligaciones, la seguridad de los datos, la evaluación de impacto, los delegados de protección de datos y los códigos de conducta y certificación.

En primer lugar, hablaremos de las obligaciones, que a partir de la entrada en vigor del RGPD serán específicas para el responsable del tratamiento de los datos, al contrario que con la LOPD, estas nuevas obligaciones consisten en mantener un registro de actividades de tratamiento, establecer medidas de seguridad aplicables al tratamiento de los datos y designar un responsable del tratamiento de los datos.

En cuanto a la seguridad de los datos, los datos deben estar protegidos desde el mismo momento en el que se diseña el tratamiento, los responsables deben tomar medidas que garanticen la seguridad de los datos desde el punto de vista de la cantidad de datos tratados, la extensión del tratamiento, los períodos de conservación y la accesibilidad a los datos. En el caso de que se produzca una violación de seguridad de los datos, ésta

[17] Seguimos en este punto la *Guía del reglamento general de protección de datos para responsables del tratamiento* publicada por la Agencia Española de Protección de Datos (2018) [online]. Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf [Acceso el 6 de marzo de 2018].

debe ser notificada a la autoridad competente en un plazo de 72 horas. Entenderemos como violación de seguridad de los datos *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos",* como define el RGPD en su artículo 4.12.

La evaluación de impacto supone elaborar un informe que valore las operaciones que se llevarán a cabo con los datos, los riesgos que existen para los derechos y libertades de los interesados, las medidas con las que se pretende hacer frente a dichos riesgos y amenazas, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales.

Sobre los delegados de protección de datos, cabe destacar, que es una nueva figura incluida en el RGPD para garantizar el cumplimiento de este. Entre sus funciones están informar, asesorar y supervisar sobre el cumplimiento del reglamento. Se nombrará un delegado de protección de datos cuando el tratamiento se lleve a cabo por un organismo público, cuando se traten datos especialmente protegidos o cuando por razón de su naturaleza, alcance los datos deban ser supervisados de forma habitual.

Por último, los códigos de conducta y certificación, el RGPD indica que serán necesarios códigos de conducta elaborados por los diferentes estados miembros para el buen funcionamiento de las leyes que dictan, estos códigos de conducta deberán tener en cuenta las necesidades de las microempresas y las pequeñas y medianas empresas. En lo que respecta a la certificación el reglamento europeo declara que los Estados miembros promoverán la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos para demostrar el cumplimiento de las normas dictadas en el Reglamento.

1.4 Problemas subsistentes

Dicho lo anterior, es complicado pensar cómo es posible que el *Big data* tenga futuro, es decir, teniendo en cuenta el Reglamento Europeo y sus restricciones, pareciera que el *Big data* es inviable, si no se pueden tratar datos personales.

Sin embargo, en el artículo 4 del Reglamento se define como interesado a la persona física identificable de manera directa o indirecta. La ley no se aplicará si no se puede identificar al individuo. El *Big data* utiliza una técnica llamada anonimización, esta técnica consiste, básicamente, en sesgar los datos para que las personas no sean fácilmente identificables, los datos anónimos quedan fuera del ámbito de aplicación del reglamento. La anonimización de datos personales consiste en delimitar y suprimir aquella información concreta que permite identificar a los individuos con el objetivo de eliminar, de forma irreversible, las posibilidades de identificación y evitar así la reidentificación cuando los datos sean reutilizados[18].

Podemos destacar, sin embargo, que la anonimización no siempre es un método fiable, en determinadas ocasiones ha resultado no ser del todo seguro, existen algunos errores comunes para tener en cuenta en los procesos de anonimización.

El primero de ellos tiene que ver con pseudonimización, una técnica que reemplaza un atributo del registro de datos por otro, la utilización de esta técnica no debe confundirse con la anonimización, ya que el interesado es se puede reidentificar, por lo que entraría de nuevo en el ámbito de aplicación del reglamento.

[18] Mediano, S. (2016). *Guía sobre los procedimientos de anonimización de datos personales*. [online] Santiago Mediano, abogados. Disponible en: http://www.santiagomediano.com/guia-sobre-procedimientos-anonimizacion-datos-personales/ [Acceso el 8 de marzo de 2018].

Otro de los errores es no tener en cuenta el impacto que puede tener la información anónima en los particulares, especialmente en el caso de los perfiles[19].

En relación con las dificultades que se nos presentan en cuanto al *Big data* y el RGPD, podemos hablar del artículo 5 del mismo, en el que se trata el principio de minimización de datos, este principio consiste en que en cualquier caso deben ser recogidos la cantidad de datos estrictamente necesarios, concretamente el reglamento habla de datos adecuados, pertinentes y necesarios, esto choca con el *Big data* que trata de analizar la mayor cantidad de datos posibles, para poder así llegar a conclusiones más acertadas.

En otro sentido el *Big data* se basa en la manipulación, es decir, hasta qué punto es lícito que se utilicen nuestros datos, o gustos para enviarnos publicidad, por ejemplo. En este aspecto cabe destacar la campaña realizada en EE.UU. en favor de Donald Trump, existe un método desarrollado por Michal Kosinski para analizar a las personas según su actividad en Facebook, Kosinski observó que se podría estar utilizando su método para que Trump ganara las elecciones, este método consiste en analizar un cuestionario que los usuarios respondían cruzando estos resultados con sus interacciones en el Facebook, extrayendo así una serie de datos que predecían de manera bastante fiable su personalidad. Esta investigación fue aplicada a la campaña de Trump, categorizando psicográficamente a los votantes para ser abordados de forma diferente. Así, se publicaban en Facebook publicaciones que solo podían ser vistas por determinados usuarios con perfiles específicos, por ejemplo, los ciudadanos afroamericanos podían ver un video en el que Hillary Clinton se refería a los hombres de raza negra como depredadores, los mensajes son diferentes solo en pequeños detalles para adaptarse de forma más concreta al perfil psicológico de los destinatarios. Existe una manipulación en este tipo de campañas, algo parecido fue utilizado también en la campaña del brexit en Europa. Cabe preguntarse si

[19] Mogollón, S. (2014). *¿Existe de verdad la Anonimización? El grupo del Artículo 29 de Protección de Datos no lo pone fácil*. [online] Noticias Jurídicas. Disponible en: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4922-iquest;existe-de-verdad-la-anonimizacion-el-grupo-del-articulo-29-de-proteccion-de-datos-no-lo-pone-facil/ [Acceso el 8 de marzo de 2018].

algo así es lícito o moral, o si existen en la legislación suficientes recursos para controlar estas situaciones[20].

1.5. En especial, en el ámbito laboral

Simultáneamente, otro de los problemas para tener en cuenta con respecto a la aparición de nuevas tecnologías son los derivados de las relaciones laborales. En este ámbito la libertad de empresa choca de manera directa con un derecho fundamental como es la intimidad.

Existe un conflicto entre el poder de dirección del empresario y la intimidad de los trabajadores, la captación de imágenes durante la jornada laboral, la escucha y grabación de conversaciones y la videovigilancia dentro y fuera de la jornada laboral, entrañan situaciones que lesionan el derecho a la intimidad del trabajador. En este sentido también podemos hablar del control que se ejerce por parte de las empresas de internet, correos electrónicos o redes sociales.

Los límites al poder de control del empresario son por un lado que la finalidad de este control sea exclusivamente laboral y por otro, que no se podrá invadir la privacidad del trabajador, entendida esta última desde el punto de vista de franjas excluidas de la prestación laboral. En cuanto al control informático la tendencia actual, teniendo en cuenta que la legislación no contempla soluciones definitivas, actualmente las empresas elaboran códigos de conductas y buenas prácticas con el fin de establecer el uso y comportamiento ante las herramientas tecnológicas que le facilitan[21].

[20] El Observador. (2017). *¿Trump ganó gracias al Big data*? [online] disponible en: https://www.elobservador.com.uy/trump-gano-gracias-al-big-data-n1023849 [Acceso el 8 de marzo de 2018].

[21] Sobre estas cuestiones, el interesante estudio de Martínez Marín, J. (2015). *El poder de dirección del empresario y el derecho a la intimidad del trabajador*. Universidad de Valladolid. (http://uvadoc.uva.es/bitstream/10324/13050/1/TFG-N.226.pdf).

2. ANÁLISIS

2.1 Derecho a la intimidad, a la protección de datos y al olvido

La protección de datos de las personas físicas es un derecho fundamental reconocido en el artículo 8 apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea[22], así como en el artículo 16 apartado 1 del Tratado de Funcionamiento de la Unión Europea. La Constitución Española[23] garantiza en su artículo 18 apartado 1 el derecho al honor, la intimidad personal y familiar y a la propia imagen. Por otro lado, el artículo 10 de la Constitución establece que los derechos fundamentales se interpretarán de conformidad con la declaración universal de los derechos humanos.

En cuanto a la protección de datos, en el ordenamiento jurídico español cabe destacar la STC 292/2000[24], fundamento jurídico 6. En esta sentencia el tribunal constitucional diferencia claramente entre el derecho a la intimidad y el derecho a la protección de datos, este último implica un derecho de hacer a un tercero, una obligación de tener un consentimiento firmado por el interesado para la recogida y uso de los datos personales, que le otorguen el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar los datos de los que hablamos. La sentencia establece que el derecho fundamental de protección de datos no se reduce solamente a los datos íntimos de una persona, sino a cualquier dato personal sea íntimo o no, al contrario que el derecho a la intimidad.

El derecho al olvido hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de

[22] Unión Europea. Carta de los derechos fundamentales de la Unión Europea. Firmada en Lisboa el 7 de diciembre de 2000 y reformada el 12 de diciembre de 2007.
[23] Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311.
[24] España. Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

La Sentencia del Tribunal Supremo 2018\38707[25] en su razonamiento jurídico tercero, relaciona el derecho al olvido con el derecho a la información, se establece como requisito indispensable en este tipo de conflictos la veracidad.

Así mismo, la sentencia del Tribunal Supremo 177/2013[26], hace referencia también al requisito de veracidad, cuando existe un conflicto entre el derecho al honor o la propia imagen y el derecho a la libertad de expresión. El requisito de veracidad no debe entenderse en términos absolutos y que puede depender de la forma en la que es presentada una noticia, el comunicador no solo debe tener en cuenta que la noticia sea verdad, sino la manera en la que la cuenta.

Los tribunales en estos casos aplican técnicas de ponderación constitucional y determinan así la prevalencia de un derecho sobre otro. En este sentido, la Sentencia 68/2000 del Tribunal Constitucional[27], en su fundamento jurídico tercero dice que las personas que ejercen cargos públicos deben soportar un mayor riesgo de intrusión en este tipo de derechos que las personas privadas.

Los poderes públicos están obligados a dar respuesta al ejercicio de los derechos de acceso, cancelación y oposición, por ello se crea la Agencia de Protección de Datos, una autoridad estatal de control independiente que se encarga de esta función en el territorio español. De las diferentes agencias estatales encargadas de la protección de datos de carácter personal, la española es la más ambiciosa al considerar que el derecho al borrado

[25] España. Auto JUR2018\38707, de 07 de febrero de 2018 del Tribunal Supremo. Recurso de casación núm. 5579/2017
[26] España. Tribunal Supremo. (Sala de lo Civil, Sala 1ª). Sentencia núm. 177/2013, de 6 de marzo de 2013.
[27] España. Tribunal Constitucional. (Sala 2ª). Sentencia núm. 68/2008, de 23 de junio de 2008.

de la información se basa en el principio del consentimiento, pero también en el de finalidad[28].

En cuanto al Derecho a la intimidad con relación al ámbito empresarial y la dependencia existente entre el trabajador y empleador, la jurisprudencia parece inclinarse por una solución salomónica: en lugar de intentar ponderar los equilibrios entre la libertad de empresa y los derechos fundamentales, que en principio gozan de mayor protección constitucional, aceptan las limitaciones de éstos en ejercicio de aquélla, siempre que 1) resulten necesarias, idóneas y proporcionales para asegurar la eficiencia productiva, y 2) se informe previamente al trabajador de las condiciones en las que esos poderes van a aplicarse y en qué medida pueden afectar a su intimidad. En este sentido, en la doctrina, los trabajos de Sánchez Trigueros[29] y López Portas[30]. Y en la jurisprudencia, la STC 3 de marzo de 2016[31] o la de 5 de septiembre de 2017 del TEDH en el célebre asunto Barbulescu vs. Rumanía.

2.2 Fueros

El crecimiento exponencial de la información que se ha producido en los últimos años ha aumentado de manera desmesurada las solicitudes de autorización de transferencias internacionales de datos personales, se solicitan datos de unos países a otros en las diferentes áreas de la sociedad recursos humanos, servicios financieros, la banca, la educación, el comercio. En materia de protección de datos, existen diferencias en la regulación en todo el mundo. Podemos identificar países o estados cuya legislación en materia de protección de datos está adaptada a la situación actual y a las nuevas

[28] López Portas, B. (2015). La protección de datos personales en el universo 3.0: El derecho al olvido de la Unión Europea tras la sentencia de TJUE de 13 de mayo de 2014. *Revista Aranzadi de Derecho y nuevas tecnologías, número 38, mayo-agosto 2015,* p. 169.
[29] Sánchez Trigueros, C. and González Díaz, F. (2011). *Libertad de empresa y poder de dirección del empresario en las relaciones laborales*. Cizur Menor: Aranzadi.
[30] Martínez Marín, J. (2015). *El poder de dirección del empresario y el derecho a la intimidad del trabajador*. Universidad de Valladolid. (http://uvadoc.uva.es/bitstream/10324/13050/1/TFG-N.226.pdf).
[31] España. Tribunal Constitucional. Sentencia 39/2016, de 8 de abril de 2016.

tecnologías, entre estos están los países miembros de la Unión Europea, Argentina, México, Canadá o Estados Unidos. Otros países se plantean mejorar su legislación en este aspecto, entre los que se pueden contar Perú, Ecuador, Colombia, Chile o Uruguay. Por último, existen algunos países que no tienen ningún tipo de normas que protejan los datos personales de sus ciudadanos, como es el caso de Rusia, Malasia o Taiwán[32].

El inconveniente de la territorialidad es especialmente importante tras la aparición de internet. Cuando nos encontramos con la vulneración de derechos personalísimos como el honor o la propia imagen, se entiende que se deberá resolver el conflicto en los lugares donde los efectos se apreciaran de manera más clara. Las grandes empresas tecnológicas pueden tener cierta fuerza con respecto a determinados países, y podrían decidir no instalar sus filiales en ellos, cuanta más fuerza tenga un territorio desde el punto de vista económico, más complicado se hará para las multinacionales no someterse a su legislación vigente[33].

El reto actual sería que hubiera una legislación mundial, pero es muy complicado por diferentes motivos, el más importante es, sin duda la falta de interés de determinados países junto con las diferencias sociales de todos ellos. Sin embargo, el RGPD es una primera piedra para llegar algún día a una regulación mundial. El hecho de que los diferentes países mundiales tengan diferentes legislaciones supone una serie de inconvenientes que de los que hablaremos a continuación.

Para empezar, uno de los problemas que se observan con las empresas que se dedican por ejemplo al tratamiento de datos, es que se pueden localizar en cualquier parte del mundo,

[32] Ortega Jiménez, A. (2014). *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. [online] Agencia Española de Protección de Datos. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/La_des_proteccion_del_titular_del_derecho.pdf [Acceso el 21 de marzo de 2018].

[33] Boix Palop, A. (2015) El equilibrio entre los derechos del artículo 18 de la Constitución, "el derecho al olvido" y las libertades informativas tras la sentencia de Google. *Revista general de Derecho Administrativo (38).*

en países que no tengan normas específicas en esta materia. Al final una empresa de este tipo no necesita una gran infraestructura, no tiene problemas en cuanto a la localización, es decir, no necesitan transportar mercancías, esto supone una gran ventaja.

Siendo así, en el artículo 2.1 de la LOPD podemos ver el ámbito de aplicación territorial de la misma. (Se aplicará hasta la entrada en vigor del reglamento europeo, en mayo de 2018.) Cuando el tratamiento se efectúe en territorio español; cuando así lo indiquen las normas de Derecho Internacional público, aunque no se traten los datos dentro del territorio español; y cuando a pesar de no estar el responsable del tratamiento dentro de la U.E. se utilice el tratamiento de datos recogidos en territorio español.

La presencia de un elemento internacional en el ámbito de la protección de datos supone un riesgo al que da respuesta el legislador. La LOPD de protección de datos se aplica según su artículo 2.1.a) cuando el responsable del tratamiento se encuentra establecido en territorio español. El apartado 2.1.c) presenta la situación de que el responsable del tratamiento de datos de carácter personal se establezca en un Estado no miembro de la Unión Europea. En este caso se puede hablar de dos diferencias, por un lado, si el responsable del tratamiento utiliza medios en España que presentan un elemento de permanencia y no simplemente de tránsito, se aplicará la Ley española. Por otro lado, si a pesar de estar en un tercer Estado, pero el responsable del tratamiento solo utiliza el Estado español como un mero tránsito de sus datos, se aplicará la ley extranjera que corresponda. Este artículo que la Ley española copia de la Directiva europea 95/46[34] pretende eliminar situaciones de riesgo para el ciudadano, cuando el responsable se establece en un Estado no miembro de la Unión Europea con el fin de eludir sus leyes. Se debe resaltar que esto es aplicable también a Noruega, Islandia y Liechtenstein.

La LOPD no dice a qué se refiere cuando habla de "un medio que no sea de mero tránsito". Un medio en España podría ser un ordenador, un terminal o un servidor. Pero "la

[34] Unión Europea. Directiva (UE) Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

utilización" se puede entender como algún tipo de actividad por parte del responsable y la intención de tratar los datos reunidos.

Se deben también tener en cuenta en las situaciones de transferencia internacional de datos de carácter personal los supuestos en los que un usuario de internet que reside en España entra en un sitio web de un empresario no establecido en la Unión Europea y envía datos a esta página, la página descarga en el disco duro español un archivo de texto, en este caso las interpretaciones indican que no es un mero tránsito, por lo que se aplicaría la LOPD. Por otro lado, se aplica la Ley del Estado miembro afectado a las aplicaciones enviadas desde una página web al ordenador del usuario cuando el responsable de los datos no establecido en un Estado miembro recaba y trata datos personales en territorio español. Los datos que un usuario español envía a un sitio web no localizado dentro de la Unión, sin que medien cookies o archivos similares, serán objeto de la Ley de ese tercer Estado[35].

"*Cuando al responsable de del tratamiento no establecido en territorio español le sea de aplicación la legislación española en aplicación de la normativa de Derecho Internacional público*". Artículo 2.1.c) de la LOPD, que hace referencia a las autoridades consulares y diplomáticas en el ejercicio de su actividad profesional. Se refiere a datos tratados en el extranjero por sujetos con capacidad para desarrollar funciones públicas. Al tratamiento de datos que hagan en el extranjero estas autoridades se le aplicará la LOPD.

El RGPD en su artículo 3, delimita el ámbito territorial del mismo, será de aplicación en los siguientes casos:

- Siempre que se traten datos personales en el contexto de las actividades de un establecimiento del responsable o encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

[35] Sancho Villa, D. (2008). Protección de Datos Personales y transferencia internacional: cuestiones de la Ley aplicable. *Revista Jurídica de Castilla y León*, 16, pp.409 a 416.

- Cuando los datos personales de los interesados que residan en la Unión sean tratados por un responsable no establecido en la Unión, siempre que las actividades estés relacionadas con la oferta de bienes o servicios de dichos interesados, sin necesidad de que se requiera un pago, o con el control de su comportamiento, en el caso de que éste tenga lugar en la Unión.
- En el caso de que el responsable trate datos personales sin estar establecido en la Unión sino en un lugar en el que sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público.

Por lo tanto, a partir del 25 de mayo de 2018, fecha de la entrada en vigor del nuevo reglamento europeo, éste será de aplicación al tratamiento de datos de todas las personas físicas de la Unión Europea, sin que sea necesario que la empresa responsable se encuentre situada dentro de la Unión y a todas las empresas que estando dentro de la Unión traten datos de ciudadanos no europeos. Queda así protegido un ámbito mucho mayor de ciudadanos en materia de protección de datos, con respecto a etapas anteriores.

Transferencia internacional de datos con EE.UU.

Entre Europa y los Estados Unidos se transfieren una gran cantidad de datos personales, es importante saber cómo afecta esto desde el legal al *Big Data*. El hecho de que ambos territorios tengan sus propias normas en materia de protección de datos ha generado un conflicto de intereses que se debe tener en cuenta.

El 29 de Julio del año 2000 se llega a un acuerdo llamado *"Safe Harvour"* o puerto seguro, este sistema permite que se intercambie información de manera continuada y estable con un rango de seguridad correcto. Muchas grandes empresas americanas utilizan este sistema. A través de este acuerdo se establecen 7 principios básicos para la protección de datos de carácter personal. Las empresas acogidas a este acuerdo establecidas en territorio norteamericano deberán notificar a los interesados sobre la recogida y posible tratamiento de estos, es necesario que los afectados tengan la posibilidad de oponerse a la recogida o tratamiento, se deberá informar al afectado cuando sus datos se trasladen a

una tercera empresa, los afectados deben poder recibir los datos que la empresa tenga de ellos para garantizar así la posibilidad de defender sus derechos cuando sea necesario[36].

Este acuerdo es aprobado a través de una decisión europea que cuenta con 6 artículos[37].

Sin embargo, este acuerdo que pretendía proteger el derecho a la intimidad de los ciudadanos ha sido invalidado por una sentencia del Tribunal de Justicia de la Unión Europea,[38] al considerar el tribunal europeo que la intimidad de los ciudadanos europeos no queda protegida con el sistema puerto seguro.

La sentencia de la que hablamos trata el caso de Scrhems, un ciudadano de nacionalidad austriaca, que reside en Austria y es usuario de la red social Facebook. Los datos personales de los usuarios de Facebook en Europa son trasladados a la sede de la empresa en EE.UU. donde son objeto de tratamiento. El interesado presenta una reclamación en la que solicita que se prohíba, en virtud de su derecho a la intimidad, que se transfieran sus datos a Norteamérica, considera que el derecho y las prácticas en vigor de este país no garantiza una protección suficiente de sus datos personales, se basa en las revelaciones de Snowden sobre las actividades de los servicios de información de los Estados Unidos.

En la sentencia la Sala del Tribunal de Justicia Europea declara inválida la decisión 2000/520, citada anteriormente, al considerar que, la decisión no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea. Las autoridades nacionales de control podrán en cualquier caso controlar la transferencia de datos a

[36] Ortega Giménez, A. (2005). *Transferencia internacional de datos de carácter personal: E.U. vs EE.UU.* [online] Disponible en: https://revistasocialesyjuridicas.files.wordpress.com/2010/09/02-tm-09.pdf [Acceso el 26 de marzo de 2018].

[37] Unión Europea. Decisión (UE, Euratom) 2000/520 Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

[38] Tribunal de Justicia de la Unión Europea. Caso (C-362/14). Sentencia de 06 de octubre de 2015.

terceros países, aunque exista una decisión europea. Sin embargo, corresponde al Tribunal de Justicia decidir si una decisión es válida o no.

La Comisión Europea a la hora de aprobar la Directiva debió llevar a cabo una investigación en la que se determine si el acuerdo conocido como "puerto seguro" cuenta con el nivel de protección adecuado, el tribunal considera que este examen no se hizo, sino que la comisión analizó el régimen de la medida. Las entidades públicas norteamericanas no se han acogido al acuerdo "puerto seguro" y solo se les aplica la Directiva a las empresas que si lo están.

Las leyes de EE. UU. prevalecen sobre la Directiva europea, por lo que en caso de conflicto serán de aplicación las primeras. Esto deriva en que los afectados no disponen de vías jurídicas para reclamar sus derechos en materia de protección de datos de carácter personal, la Decisión de la Comisión no especifica si en el territorio estadounidense existen normas que limiten los posibles conflictos que surgen en estos casos.

Para resumir, las leyes en materia de seguridad ciudadana de los EE. UU. permiten que las autoridades puedan acceder a todos los datos, de este modo, los datos de ciudadanos europeos, recogidos en Europa pueden ser tratados y observados por los Estados Unidos.

El Tribunal considera que la Decisión no es válida ya que se limita a una serie de artículos, autoriza de manera generalizada la conservación de la totalidad de los datos personales, sin establecer diferenciación, limitación o excepción en función del objeto perseguido.

Por último, el Tribunal señala que las autoridades nacionales pierden competencias de control con la Decisión 2000/520 en el caso de que un interesado impugne la compatibilidad de la Decisión con la protección de la vida privada y de las libertades y derechos fundamentales[39].

[39] Ídem.

El traslado de datos entre empresas europeas y norteamericanas es totalmente necesario en un mundo cada vez más globalizado, tras la sentencia del Tribunal Europeo que declaraba inválida la Directiva 2000/520 se han generado una serie de problemas, el puerto seguro ya no es una opción y se hizo necesario buscar nuevas soluciones. En el año 2016 se aprobó un nuevo acuerdo llamado escudo de privacidad para la transmisión de datos entre Europa y Estados Unidos.

El marco del "escudo de privacidad" obliga al Departamento de Comercio de los Estados Unidos a llevar a cabo actualizaciones y revisiones periódicas de las empresas que se acojan al acuerdo garantizando así que se cumpla la normativa establecida[40].

Para poder llegar a este acuerdo ha sido necesario imponer límites a las autoridades estadounidenses en relación con su ley de seguridad nacional. La Oficina del Director de Inteligencia Nacional asegura que la recopilación en bloque de datos solo podrá ser utilizada en condiciones específicas y predeterminadas y tiene que ser lo más concreta y precisa posible. Se ha establecido un recurso en el ámbito de la inteligencia nacional para los europeos a través de la figura del Defensor del Pueblo en el departamento de Estado[41].

La vulneración de los derechos de los ciudadanos se resolverá por medio de la resolución de litigios accesibles y asequibles, la Comisión Europea en su nota de prensa establece que lo ideal sería que las empresas resolvieran estos conflictos, pero en caso de negativa, se facilitará a los ciudadanos mecanismos gratuitos. Los afectados podrán dirigirse a sus autoridades nacionales de protección de datos, que en colaboración con la Comisión Federal de Comercio garantizará la investigación y resolución. En última instancia conocerá del asunto el Defensor del pueblo[42].

Por último, es necesario un seguimiento del funcionamiento del "escudo de privacidad", un examen en el que expertos nacionales de inteligencia de Estados Unidos y las

[40] European Commission. Press Realease Database. (2016). *La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos*. [online] Disponible en: http://europa.eu/rapid/press-release_IP-16-2461_es.htm [Acceso el 26 de marzo de 2018].
[41] Ídem.
[42] Ídem.

autoridades europeas, basándose en todas las fuentes de información deberán decidir si se han cumplido los compromisos y garantías[43].

La AEPD ha elaborado una guía sobre el escudo de privacidad[44]. En esta guía se examinan las obligaciones de las empresas y los derechos de los ciudadanos, el procedimiento para presentar una queja contra una empresa y el mecanismo Ombudsperson para interponer un procedimiento frente a las autoridades estadounidenses.

Según esta guía, las empresas que se acojan al acuerdo "escudo de privacidad" se verán obligadas a informar a sus usuarios sobre los datos con los que trabajan y los motivos de su tratamiento, si tiene intención de transferir a una tercera empresa sus datos y por qué. Los usuarios, por su parte tendrán derecho a solicitar a la empresa el acceso a sus datos personales, a decidir si permite si sus datos personales pueden ser transferidos a otra empresa, "derecho de exclusión voluntaria". La empresa tiene el deber de informar a los usuarios sobre cómo ponerse en contacto con la misma en caso de que el usuario tenga dudas sobre sus datos de carácter personal, también deberán informarles sobre el órgano de resolución de conflictos al que podría presentar su caso y sobre la opción de que la empresa tenga que responder ante las Autoridades de los Estados Unidos en caso de revelar por Ley información acerca del usuario.

No se permitirá usar sus datos para fines incompatibles con los fines firmados previamente, si se trata de un fin sustancialmente distinto, pero que guardar relación con el original, la empresa solo podrá utilizarlos si el usuario no pone objeciones, en caso de que los datos sean especialmente sensibles, el usuario tendrá que dar su consentimiento explícito.

Para el buen funcionamiento del acuerdo "escudo de privacidad" las empresas deberán tratar los datos únicamente para los fines que fueron recogidos, no permitiéndose guardar estos datos posteriormente, salvo en los casos en que sea necesario por motivos de interés

[43] Ídem.

[44] Agencia Española de Protección de datos. (2016). *GUÍA ACERCA DEL ESCUDO DE PRIVACIDAD UE - EE. UU.*[online] Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Guia_acerca_del_Escudo_de_Privacidad.pdf [Acceso el 26 de marzo de 2018].

público, periodismo, literatura y arte, investigación científica o histórica o para el análisis estadístico. Los datos deberán guardarse en un entorno seguro y protegerse frente a la pérdida, utilización ilegal, accesos no autorizados, revelación, alteración o destrucción.

En el caso de que las autoridades de Estados Unidos accedan a la información del usuario de una empresa sujeta al acuerdo de "escudo de privacidad", el acuerdo asegura que esto solo se dará en el caso de que sea necesario para la seguridad nacional. En caso de que accedan, existe un mecanismo para resolverlo que se llama "Ombudsperson". Se trata de un mecanismo propuesto por el escudo de privacidad que cubre todos los tipos de reclamaciones que tengan que ver con transferencias comerciales de la Unión Europea a empresas de los Estados Unidos.

2.3 Consentimiento

El consentimiento es considerado como derecho fundamental de los ciudadanos, se establece así en el artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea[45]. Este artículo determina que los datos podrán ser tratados sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la ley.

Como ya se ha dicho a lo largo del trabajo el *Big data* consiste en el tratamiento masivo de datos, para poder tratar los datos de carácter personal, es necesario según el artículo 6 de RGPD el consentimiento del interesado. El consentimiento es un elemento fundamental en el tratamiento de datos. Sin contar con el consentimiento, en determinadas ocasiones se puede llevar a cabo el tratamiento de datos de carácter personal, cuando se de alguna de las siguientes circunstancias:

- Que el tratamiento sirva para ejecutar un contrato en el que el interesado sea una de las partes.

[45] Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea, firmada en Estrasburgo el 12 de diciembre de 2007. Diario Oficial de la Unión Europea C 303 de 14 de diciembre de 2007.

- Que para cumplir una obligación legal sea indispensable el tratamiento de los datos.
- Que el tratamiento se necesite para cumplir un interés vital del interesado.
- Que en virtud del interés público los datos deban ser tratados.
- Que sea necesario el tratamiento para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

La Unión Europea define en el artículo 4.11 del RGPD el consentimiento 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".*

El artículo 7 del RGPD, establece las condiciones para el consentimiento, la primera de ellas es que el responsable del tratamiento pueda demostrar el consentimiento, la segunda, en la solicitud de consentimiento se deberán distinguir claramente los diferentes asuntos, de forma inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. En tercer lugar, el interesado tendrá derecho a retirar su consentimiento en cualquier momento. Por último, el reglamento pone como condición para el consentimiento que éste se dé libremente. A la hora de ejecutar un contrato se deberá tener en cuenta si se supedita al consentimiento del tratamiento de datos personales que no son necesarios para llevarlo a cabo.

El consentimiento en las cookies.

Qué pasa con las *cookies,* al entrar en una página web, muchas veces se nos informa de la utilización de esta tecnología, con una ventana emergente que nos da la opción solo de aceptar, esto ha sido posible porque hasta ahora se podía considerar que al entrar en la página estábamos, de manera implícita, aceptando su uso.

Las *cookies*[46] son archivos que se almacenan en el dispositivo que estamos utilizando sobre las páginas que visitamos, esto facilita la publicidad teniendo en cuenta nuestras preferencias. En el año 2009, la Unión europea aprueba una Directiva[47] que regula el uso de las cookies, en España existe la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico[48], en el artículo 22 de la misma se establece la necesidad de que el usuario sea informado sobre el uso de dispositivos de almacenamiento y recuperación de datos, como son las cookies, y su finalidad.

La directiva 2002/58[49], establecía que, como hemos dicho antes, la entrada en la web a pesar de la información del uso de *cookies* implicaba aceptar la condición de que se están utilizando, si le interesa el sitio web sabiendo que utiliza la política de *cookies* acepta descargar el contenido, esta Directiva por lo tanto reconoce la posibilidad de que los editores de cada página, solo informando de su uso puedan utilizar las *cookies.* En su artículo 5.3, la Directiva establece la obligación de informar al interesado y de ofrecerle un medio para poder oponerse a la instalación de *cookies,* pero, además, obliga a los editores a que exista un consentimiento de una solicitud previa de autorización.

Esta nueva legislación ha supuesto algunos problemas de interpretación, por un lado, el artículo 66 de la Directiva 2009/136[50] solo habla del derecho de oposición de una forma

[46] Méndez, L. (2013). ¿Qué son las cookies? *Escritura pública*, [online] (82), pp.16-18. Disponible en: http://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-110181.pdf [Acceso 23 Abril. 2018].

[47] Unión Europea (UE) 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

[48] España. Ley 34/2002, de 11 de julio, de servicios de la sociedad de información y de comercio electrónico. Boletín Oficial del Estado, 12 de Julio de 2002, núm.166.

[49] Unión Europea. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas (Directiva sobre la Privacidad y las Comunicaciones Electrónicas). Diario Oficial n° L 201, de 31 de julio de 2002.

[50] Unión Europea. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE Relativa al Servicio Universal y los Derechos de los Usuarios en Relación con las Redes y los Servicios de Comunicaciones Electrónicas, la Directiva 2002/58/CE Relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el

muy poco tajante, en ningún momento se establece la obligación de consentimiento expreso por parte del usuario. El artículo 5.3 modificado hace referencia al consentimiento explícito que solo será evitable en el caso de que el navegador esté configurado para aceptar las *cookies.*

El grupo de trabajo del artículo 29, en su Directiva 2/2010 dispone que se deberá aceptar previamente y de forma explícita el uso de las *cookies* antes de que el paquete sea instalado en el equipo. El grupo de trabajo del artículo 29 en su Directiva 4/2010 asegura que el sistema de oposición no cumple el requisito temporal, las *cookies* son instaladas antes de darnos la opción de negarnos, desde que entramos en el sitio web. [51]

Por otro lado, el Grupo de Trabajo del Artículo 29 afirma que la oposición resultaría válida solamente en el caso de que el usuario tenga suficiente conocimiento del uso de las *cookies* y en no en general para todos los usuarios.

En cuanto a la configuración del navegador, se hace complicada esta opción, ya que los navegadores, pueden estar, por defecto, configurados para aceptar las *cookies*, por lo tanto, para poder validar esta opción es necesario que el navegador esté configurado de manera general para no aceptarlas, de tal forma que sea el usuario el que deba reconfigurar su navegador. También se entiende que la configuración del navegador no puede ser definitiva, ya que el usuario no sabe qué está aceptando, qué paquetes se descargarán en un futuro. Se recomienda desde el Grupo de Trabajo del Artículo 29 que el permiso no sea definitivo y las *cookies* caducaran en un año. Se propone el uso de iconos en los sitios webs que recuerden de manera permanente al usuario que se están utilizando *cookies.* Todos los organismos implicados en la instalación y explotación de la *cookie* están obligados a respetar las garantías aplicables a su caso[52].

Sector de las Comunicaciones Electrónicas y el Reglamento (CE) no 2006/2004 Sobre la Cooperación en Materia de Protección de los Consumidores. Diario Oficial n° L 337, de 18 de diciembre de 2009.

[51] Salom, J. A., & Tomé, S. S. (2014). El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos. *Revista Aranzadi Doctrinal*, (11), 217-235.

[52] Ídem.

"Una cookie puede utilizarse para diversas finalidades, por lo que únicamente podrá estar exento del requisito del consentimiento si todas y cada una de las finalidades para las que se utilice están individualmente exentas del requisito del consentimiento"[53].

Sin embargo, existe una excepción, se puede hacer uso de las cookies sin consentimiento siempre que se utilicen con el único fin de transmitir una comunicación o en el caso de que sea una condición indispensable para la prestación de un servicio solicitado por el destinatario. Según el grupo de trabajo del Artículo 29 se interpretaría que el usuario al entrar en la página está solicitando la prestación de un servicio y, por tanto, se podrían utilizar las cookies sin aceptar el consentimiento.

El Real Decreto-ley 13/2012[54], establece las obligaciones de información al exigir un consentimiento previo como requisito para la legitimidad de la instalación de las cookies, no obstante, no indica quién debe ser el responsable de avisar sobre las cookies a los usuarios, del mismo modo, no señala quién será el encargado del tratamiento ni de la gestión de los datos personales obtenidos o qué derivaciones legales tendrá el incumplimiento de la normativa[55].

Permisos de las aplicaciones

En el mes de marzo de 2013 se aprobó el primer dictamen conjunto sobre aplicaciones móviles, desarrollado por el grupo de trabajo del artículo 29[56], a continuación, se

[53] Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies, adoptado el 7 de junio de 2012 (WP 194), página 6.
[54] España. Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista.
[55] Martínez Pastor, E. y Múñoz Saldaña, M.: «En busca de equilibrio entre la regulación y la autorregulación de la publicidad comportamental en línea», Estudios sobre el mensaje periodístico, vol.19, marzo, Universidad Complutense, Madrid, 2013, p. 292 (http://revistas. ucm.es/index.php/ESMP/article/viewFile/42036/40017).
[56] Agencia española de protección de datos. (2013). *Las Autoridades europeas de protección de datos aprueban el primer dictamen conjunto sobre aplicaciones móviles*. [online] Disponible en:

expondrán las partes más importantes del mismo. Los usuarios de smartphones y tabletas descargan una media de 37 aplicaciones al año y en las tiendas de aplicaciones se reciben cerca de 1600 aplicaciones nuevas cada día (datos de 2013). Las aplicaciones suponen un gran riesgo respecto a la privacidad, muchas de ellas al descargarse nos piden permisos para acceder a la localización, la cámara, la agenda, etc.

En el dictamen aprobado por las autoridades europeas en materia de protección de datos se establecen las obligaciones de los desarrolladores y de los demás participantes en el desarrollo y distribución de estas. Es especialmente importante, según se informa en el Dictamen obtener el consentimiento informado y previo del usuario. En cuanto al conflicto con normas de estados, cabe destacar que será utilizado el Reglamento Europeo de protección de datos, siempre que los terminales de los usuarios estén establecidos en la Unión Europea.

Las diferentes aplicaciones pueden recopilar enormes cantidades de datos relacionados con la ubicación, las cámaras, agendas y demás, lo que supone un grave riesgo para la intimidad de los usuarios, se hace necesario el cumplimiento de la normativa para proteger la intimidad de la población en la medida de los posible.

Para proteger la privacidad, el dictamen hace hincapié en la necesidad de que se lleve a cabo a la hora de descargar la aplicación un consentimiento informado previo, el dictamen manifiesta que no todas las aplicaciones informan adecuadamente sobre el tipo de datos que la aplicación puede recoger ni con qué fines. El consentimiento, imprescindible para el tratamiento de datos de carácter personal, muchas veces se limita a ofrecer al usuario una opción que solo permite aceptar los términos y condiciones aplicables. El grupo de Trabajo del Artículo 29 propone que los usuarios puedan controlar sus propios datos personales, los desarrolladores de las apps deben ofrecer información suficiente sobre los datos que van a tratar antes de hacerlo, obteniendo así un consentimiento válido. El Grupo destaca la necesidad de que exista una opción para cancelar la instalación si no estamos de acuerdo con las condiciones.

---

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/marzo/130314_NP_Dictamen_aplicaciones.pdf [Acceso 9 de Mayo 2018].

El usuario tiene que poder conocer qué datos está cediendo y porqué. El dictamen también considera importante la finalidad de los datos recogidos, dejando clara la necesidad de que se defina no solo qué datos serán recogidos sino también para qué serán utilizados, si se cederán a otras empresas y la forma a través de la que el usuario podría revocar su consentimiento y eliminar sus datos.

Una vez desinstalada una aplicación, el creador del sistema operativo debe avisar al desarrollador de que la app, porque legalmente no debe seguir tratando los datos de ese usuario.

Existen infinidad de aplicaciones destinadas a menores, en España no es posible tratar datos de menores de 14 años sin el consentimiento de sus tutores legales, pero se recomienda a los desarrolladores que tengan en cuenta las diferentes legislaciones en los distintos estados miembros. Se considera a los menores un colectivo especialmente sensible y vulnerable por lo que no sería apropiado utilizar los datos para fines publicitarios. Los términos y condiciones legales de las aplicaciones destinadas a este colectivo deberán estar redactadas de manera sencilla y con un lenguaje que puedan entender.

2.4 Sanciones

En cuanto a las sanciones es importante destacar que tanto la LOPD como el RGPD, establecen sanciones para las empresas que incurran en irregularidades legislativas en materia de protección de datos personales, calificando las infracciones como leves, graves o muy graves.

En la siguiente tabla podemos observar cómo el RGPD es mucho más restrictivo que la LOPD estableciendo sanciones más duras por las mismas infracciones, con lo que se pretende incentivar a las empresas para que cumplan con la normativa, ya que la dureza de las sanciones puede determinar el devenir de una empresa. Sin embargo, la tabla no está completa, ya que en los artículos 83.4 y 83.5 del RGPD se establece que si el 2%, en caso de sanciones graves, o el 4%, en caso de sanciones muy graves, son superiores a las cantidades indicadas se aplicarán estos porcentajes como sanción.

[57]

El código penal[58] en los artículos 278 a 281 contempla una pena privativa de libertad o de prisión de 2 a 4 años y multa de 12 a 24 meses, en el caso de que se hayan descubierto secretos apoderándose de datos o soportes. Igualmente, y para el caso de difusión, revelación o cesión a terceros de los secretos descubiertos mediante el acceso a los datos, el tipo penal establece pena de prisión de 3 a 5 años y multa de 12 a 24 meses, por lo que también en este caso ya ha sido vulnerado el derecho a la intimidad.

En ambos casos, y en el de las sanciones administrativas, el usuario ya ha sido perjudicado al haberse vulnerado su intimidad. De ser posible ejercitar acciones penales, la sentencia condenatoria dictará la indemnización civil pertinente o bien la misma será determinada en la ejecución de la misma, sin embargo considero que, probablemente, la única vía de

[57] Vázquez, S. y De Miguel, J. (n.d.). *Nuevo régimen sancionador de protección de datos*. [online] Ecija.com. Available at: https://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf [Acceso 5 de mayo de 2018].

[58] España. Ley orgánica 10/1995, de 23 de noviembre, del Código penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281.

la que dispone, la persona física o jurídica perjudicadas, tras una sanción administrativa por aplicación del reglamento, es la de interponer la correspondiente demanda en la jurisdicción civil ejercitando una acción de reclamación de indemnización por daños y perjuicios y, acumuladamente, la acción de reclamación de otra indemnización por lucro cesante, ésta última si la vulneración de este derecho acarreare también un perjuicio económico objetivamente valorable. Evidentemente, se revela la dificultad de cómo valorar la indemnización por daños y perjuicios dado el componente subjetivo de la misma, no así la indemnización por el lucro cesante, que sí es objetivable.

El usuario ya ha sido perjudicado en estos casos y por lo tanto tendrá derecho a interponer una reclamación solicitando una indemnización por daños y perjuicios, como se establece en el artículo 82.1 del RGPD. En la sentencia del Tribunal Supremo del 27 de junio de 2016[59], la empresa Orange había sido demandada por un usuario ya que lo habían incluido en una lista de morosos, la sentencia diferencia en su fundamento jurídico 3 entre la indemnización por daños y las indemnizaciones simbólicas, estas últimas no caben en este tipo de procedimientos, como se ha dictado en otras sentencias del mismo tribunal, en el fundamento jurídico 4 se habla de la importancia de la difusión de los datos, si han sido publicados o no.

Con respecto a los derechos de supresión y bloqueo de los datos, los artículos 12.b y 14.a de la Directiva 95/46[60] nos indican que el interesado puede dirigirse a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas webs, para que dicha información no sea conocida por los internautas, al considerar que puede perjudicarle. Del conjunto de consideraciones referidas a la segunda cuestión perjudicial de la Sentencia de Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014[61], debe extraerse, que la actividad de un motor de búsqueda que consiste en hallar

[59] España. Tribunal Supremo (Sala de lo Contencioso, Sección 6ª). Sentencia núm. 3048/2016, de 27 de junio de 2016.
[60] Unión Europea. Directiva (UE) Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
[61] Tribunal de Justicia de la Unión Europea. Caso (C-131/12). Sentencia de 13 de mayo de 2014.

información publicada en internet por terceros, indexarla, almacenarla y ponerla a disposición de los usuarios según un orden de preferencia determinado, debe calificarse como tratamiento de datos personales y por lo tanto el motor de búsqueda debe ser considerado como responsable.

Por último, el usuario en caso de que se hayan publicado datos que considere privados y que no desee que se conozcan podrá ejercer el derecho de supresión o derecho al olvido, para ello es necesario que el usuario se dirija al buscador que deben tener un formulario que permita ejercitar el derecho, si no hay respuesta o no es la que esperaba, puede reclamar ante la AEPD.

2.5 Caso Facebook

Mark Zuckerberg el fundador, presidente, dueño y consejero delegado de la empresa Facebook ha reconocido públicamente la filtración masiva de datos personales de los usuarios de esta compañía. En los últimos meses hemos escuchado en todos los medios de comunicación muchas noticias sobre esta filtración de datos, parece que en EE.UU. el gran problema es la influencia que pueden haber tenido en la elección del presidente Trump. Aún es imposible saber cómo afectará a Facebook esta situación, ya que se está investigando.

Por otro lado, la empresa Facebook está siendo investigada en Reino Unido debido a la filtración masiva de datos y su posible relación con la campaña del Brexit.

En cuanto a las prácticas, poco ajustadas al derecho de la Unión Europea, que Facebook en materia de protección de datos es importante señalar el caso de Facebook Ireland, en el que un joven, Max Schrems, denuncia a la compañía Facebook por la cesión de datos a EE.UU. de las filiales en Europa, se rompe así con el hasta entonces válido acuerdo de puerto seguro[62].

[62] Tribunal de Justicia de la Unión Europea. Caso (C-362/14). Sentencia de 06 de octubre de 2015.

En octubre de 2016, la AEPD inicia de oficio un procedimiento con el fin de investigar las comunicaciones de datos personales entre Facebook y WhatsApp. Tras la resolución dictada el 15 de marzo de 2018[63], de la que se seguirá hablando a lo largo de este epígrafe, hemos conocido que ambas empresas han sido sancionada a abonar 300.000 € respectivamente[64].

La empresa de mensajería WhatsApp fue adquirida por Facebook en 2014, en 2016 hay un cambio en la política de privacidad que permite compartir la información de los usuarios entre las dos aplicaciones.

Se establecen como hechos probados en la resolución que la compañía WhatsApp facilita a Facebook datos personales de los usuarios infringiendo el artículo 11.1 de la LOPD, a pesar de existir un consentimiento de los términos y condiciones legales, en la resolución no se entiende que este sea libre, lo que impide que pueda considerarse válido. En la política de privacidad de WhatsApp se informa que la aplicación recibe o recopila información de sus usuarios. Esta información incluye la cuenta del usuario, pero también su número de teléfono móvil, la agenda, nombre, foto de perfil y mensaje de estado. Recopilan información sobre los dispositivos del usuario, las cookies, estados de conexión y última conexión. En cuanto al terminal, cuenta con información como la dirección IP, información de la red móvil y ubicación del dispositivo.

Por otra parte, la política de privacidad de WhatsApp informa de que puede recopilar información del usuario proporcionada por terceros, a través, por ejemplo, de las agendas de otros usuarios.

[63] Agencia Española de Protección de Datos. Procedimiento Nº PS/00219/2017. Resolución: R/00259/2018. 2 de marzo de 2018. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2018/common/pdfs/PS-00219-2017_Resolucion-de-fecha-02-03-2018_Art-ii-culo-11-6-LOPD.pdf [Acceso 11 de mayo de 2018].

WhatsApp no indica que estos datos no se cederán a Facebook, sino que no serán visibles para el resto de los usuarios. Facebook utiliza los datos de los usuarios de WhatsApp con un fin específico y para el beneficio de su propia actividad. Simplemente asegurar compartir información con la finalidad de ayudar, proveer, mejorar, entender, personalizar y comercializar sus ofertas, para que el usuario pueda tener una mejor experiencia, para mostrar sugerencias de productos y mostrar ofertas o publicidad que puedan ser de su interés.

La AEPD resuelve sancionar a Facebook con 300.000, por la infracción del artículo 6 de la LOPD, relativo al consentimiento, ya que este se entiende que no es válido, esta infracción está tipificada como grave en el artículo 44.3.b de la propia Ley.

Así mismo, la compañía WhatsApp es también sancionada porque cede datos personales a otra entidad para fines que no están relacionados de manera directa con las funciones de esta aplicación, lo que supone una violación del artículo 11 de la LOPD, infracción grave artículo 44.3. k.

Por otro lado, la empresa está siendo investigada en Reino Unido debido a la filtración masiva de datos y su posible relación con la campaña del Brexit.

3. CONCLUSIONES

El *Big data* implica un análisis masivo de datos que representa un riesgo para la población en cuanto a su confidencialidad y privacidad. La aparición y utilización de nuevas tecnologías como internet, inteligencia artificial o el internet de las cosas, nos hace la vida más fácil. En función de nuestras preferencias y a través de estas, recibimos recomendaciones sobre dónde ir a cenar, nos recuerdan si tenemos programado un viaje, o si ha ganado nuestro equipo favorito. Sin embargo, la aparición de estas nuevas tecnologías hace cada vez más complicada la protección del derecho a la intimidad. Los datos que se utilizan podrían ser personales, tanto los escritos que contengan aspectos privados, como los que puedan reflejar la propia imagen, fotografías, videos, etc., lo que se traduce en un riesgo para la intimidad de los usuarios.

La Constitución española contiene una serie de derechos programáticos fundamentales entre ellos el derecho a la intimidad y el derecho a la información, cuyo desarrollo se hace efectivo mediante leyes orgánicas y reglamentos. Podemos observar que existe una colisión de derechos entre ambos. Tratándose de dos derechos fundamentales es muy difícil determinar o situar uno por encima del otro, por lo que dependerá de cada situación concreta. En cualquier caso, son derechos no negociables, salvo que una persona en un acto jurídico documentado renuncie total o parcialmente.

El RGPD implica un avance con respecto a la legislación actual, supone la unificación de derechos en la comunidad europea y establece importantes modificaciones en lo que se refiere al tratamiento y la libre circulación de datos de carácter personal. Sin embargo, en ningún caso puede garantizar el derecho a la intimidad. El nuevo reglamento europeo presenta una particularidad importante, al contrario que las legislaciones anteriores, establece los datos que pueden ser tratados y cómo, favoreciendo así la explotación de estos. Parece evidente que los propios Estados tienen interés directo en que se siga comercializando con información que a su vez se traduce en más poder, tanto sobre los ciudadanos como sobre las propias empresas.

En lo que se refiere al ámbito laboral y la utilización de las tecnologías, la voluntariedad desaparece debido a la relación de dependencia entre el empresario y el trabajador. Parece que, en el ámbito empresarial, el límite está puesto en la información y consentimiento firmado del trabajador, en favor de la libertad empresarial. En este sentido el análisis de los datos digitales generados por el trabajador, o la toma de decisiones de las empresas basándose en lo que los trabajadores publican en sus redes sociales constituyen un grave riesgo para la intimidad de este último.

Actualmente, se está produciendo una transformación social que se traduce en el cambio del concepto de derecho a la intimidad como lo habíamos entendido hasta el momento, el uso cada vez más temprano de móviles, ordenadores portátiles o tabletas está condicionando a las nuevas generaciones con una gran rapidez. El acceso a internet desde dispositivos móviles sin control contribuye a crear una sociedad despreocupada, indiferente y apática en quienes la integran, cuestión que traspasa las fronteras nacionales, hasta convertirse en un problema global. La despreocupación de la población en lo que se refiere a sus datos personales es evidente y lo que antes se podía considerar íntimo o personal, cada vez lo es menos. ¿Podríamos concluir entonces que nos estamos dirigiendo hacia un mundo en el que el derecho a la intimidad no será fundamental y por lo tanto intocable?

La continua aceptación que se nos exige en políticas de privacidad en redes sociales, aplicaciones o cookies nos acabará convirtiendo en autómatas que habrán renunciado casi por completo, o en gran parte a su derecho a la intimidad. En este sentido, autores como Aldous Huxley, en su novela “Un mundo feliz”, retrataron, muy anticipadamente a su tiempo, concretamente en el inicio de la década de los años 30 del siglo pasado, una sociedad sin libre voluntad en sus integrantes, con personas que no eran dueñas de sus vidas, llegando al punto de carecer de derechos como la libertad sexual, la decisión de la elección de sus horas de ocio, la libertad en cuanto a la gestación e incluso con quién y renunciando, en general, a su propia voluntad.

4. BIBLIOGRAFÍA

- Ferrer-Sapena, A., & Sánchez-Pérez, E. (2013). Open data, Big data: ¿Hacia dónde nos dirigimos? *Anuario ThinkEPI 2013*, *7*, 150-156.
- Sancho Villa, D. (2008). Protección de Datos Personales y transferencia internacional: cuestiones de la Ley aplicable. *Revista Jurídica de Castilla y León*, 16, pp.409 a 416.
- Salom, J. A., & Tomé, S. S. (2014). El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos. *Revista Aranzadi Doctrinal*, (11), 217-235.
- Méndez, L. (2013). ¿Qué son las cookies? *Escritura pública*, (82), pp.16-18.
- Berrrocal Lanzarot, A. (2017). *Derecho de supresión de datos o derecho al olvido*. 1ª ed. Madrid: Reus, S.A., pp. 214-215
- López Portas, B. (2015). La protección de datos personales en el universo 3.0: El derecho al olvido de la Unión Europea tras la sentencia de TJUE de 13 de mayo de 2014. *Revista Aranzadi de Derecho y nuevas tecnologías, número 38, mayo-agosto 2015,* p.169.
- Martínez Pastor, E. y Múñoz Saldaña, M.: «En busca de equilibrio entre la regulación y la autorregulación de la publicidad comportamental en línea», Estudios sobre el mensaje periodístico, vol.19, marzo, Universidad Complutense, Madrid, 2013, p. 292 (http://revistas. ucm.es/index.php/ESMP/article/viewFile/42036/40017).
- Boix Palop, A. (2015) El equilibrio entre los derechos del artículo 18 de la Constitución, "el derecho al olvido" y las libertades informativas tras la sentencia de Google. *Revista general de Derecho Administrativo (38).*
- Martínez Marín, J. (2015). *El poder de dirección del empresario y el derecho a la intimidad del trabajador*. Universidad de Valladolid. (http://uvadoc.uva.es/bitstream/10324/13050/1/TFG-N.226.pdf).
- Sánchez Trigueros, C. and González Díaz, F. (2011). *Libertad de empresa y poder de dirección del empresario en las relaciones laborales*. Cizur Menor: Aranzadi.

Jurisprudencia:

- España. Auto JUR2018\38707, de 07 de febrero de 2018 del Tribunal Supremo. Recurso de casación núm. 5579/2017.
- España. Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- España. Tribunal Supremo (Sala de lo Contencioso, Sección 6ª). Sentencia núm. 3048/2016, de 27 de junio de 2016.
- España. Tribunal Supremo. (Sala de lo Civil, Sala 1ª). Sentencia núm. 177/2013, de 6 de marzo de 2013.
- España. Tribunal Constitucional. (Sala 2ª). Sentencia núm. 68/2008, de 23 de junio de 2008.
- España. Tribunal Constitucional. Sentencia núm. 39/2016, de 8 de abril de 2016.
- Agencia Española de Protección de Datos. Procedimiento N.º PS/00219/2017. Resolución: R/00259/2018. 2 de marzo de 2018.
- Tribunal de Justicia de la Unión Europea. Caso (C-362/14). Sentencia de 06 de octubre de 2015.
- Tribunal de Justicia de la Unión Europea. Caso (C-131/12). Sentencia de 13 de mayo de 2014.

Legislación:

- España. Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311.
- España. Ley Orgánica 14/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 13 de diciembre de 1999, num 298.

- España. Ley 34/2002, de 11 de julio, de servicios de la sociedad de información y de comercio electrónico. Boletín Oficial del Estado, 12 de Julio de 2002, núm.166.
- España. Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado, 14 de mayo de 1982.
- España. Ley Orgánica 10/1995, de 23 de noviembre, del Código penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281.
- España. Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista.
- Unión Europea. Directiva (UE) Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Unión Europea. 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).
- Unión Europea. Carta de los derechos fundamentales de la Unión Europea. Firmada en Lisboa el 7 de diciembre de 2000 y reformada el 12 de diciembre de 2007.
- Unión Europea. Decisión (UE, Euratom) 2000/520 Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

- Tribunal de Justicia de la Unión Europea. Caso (C-362/14). Sentencia de 06 de octubre de 2015.
- Unión Europea (UE) 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.
- Unión Europea. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas (Directiva sobre la Privacidad y las Comunicaciones Electrónicas). Diario Oficial núm. L 201, de 31 de julio de 2002.
- Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies, adoptado el 7 de junio de 2012 (WP 194), página 6.

Recursos online:

- Espinoza Paredes, S. (2015). Generar un marco de referencia para implementaciones de Big Data para telecomunicaciones, caso de estudio corporación nacional de telecomunicaciones. [online] Disponible en: http://dspace.udla.edu.ec/bitstream/33000/3419/1/UDLA-EC-TMGSTI-2015-17%28S%29.pdf
- Www-01.ibm.com. (2018). *IBM – Big Data - Argentina*. [online] Disponible en: https://www-01.ibm.com/software/ar/data/bigdata/
- Domo.com. (2017). *Data Never Sleeps 5.0 | Domo*. [online] Disponible en: https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1

- CISCO, Cloud Index White Paper, 2013-2018. [online] Disponible en: www.terena.org/mail-archives/storage/pdfVVqL9tLHLH.pdf
- Mallol, E., Plasencia, A. and S.L.U., U. (2018). 'Debes saber que si un servicio es gratuito el producto eres tú'. [online] ELMUNDO. Disponible en: www.elmundo.es/economia/2014/11/28/547772eee2704e295e8b457d.html
- Sánchez Barroso, M. (2016). *Iniciando el camino para cumplir con la nueva Regulación Europea de Protección de Datos*. [online] SSa Asesores. Disponible en: https://ssa-asesores.es/html/wordpress/blog/2016/05/19/iniciando-el-camino-para-cumplir-con-la-nueva-regulacion-europea-de-proteccion-de-datos/
- García Martín, I. (2016). *Nuevo derecho reconocido por el Reglamento Europeo de Protección de Datos; "Limitación del Tratamiento"*. [online] Picón y asociados, abogados. Disponible en: https://www.piconyasociados.es/noticias/nuevo-derecho-reconocido-por-el-reglamento-europeo-de-proteccion-de-datos-limitacion-del-tratamiento/
- Mediano, S. (2016). *Guía sobre los procedimientos de anonimización de datos personales*. [online] Santiago Mediano, abogados. Disponible en: www.santiagomediano.com/guia-sobre-procedimientos-anonimizacion-datos-personales/
- Mogollón, S. (2014). *¿Existe de verdad la Anonimización? El grupo del Artículo 29 de Protección de Datos no lo pone fácil*. Noticias Jurídicas. Disponible en: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4922-iquest;existe-de-verdad-la-anonimizacion-el-grupo-del-articulo-29-de-proteccion-de-datos-no-lo-pone-facil/
- El Observador (2017). *¿Trump ganó gracias al Big data*? [online] disponible en: https://www.elobservador.com.uy/trump-gano-gracias-al-big-data-n1023849
- Ortega Giménez, A. (2005). *Transferencia internacional de datos de carácter personal: E.U. vs EE.UU.* [online] Disponible en: https://revistasocialesyjuridicas.files.wordpress.com/2010/09/02-tm-09.pdf

- Vázquez, S. y De Miguel, J. (n.d.). *Nuevo régimen sancionador de protección de datos*. [online] Ecija.com. Available at: https://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf [Acceso 5 de mayo de 2018].
- European Commission. Press Realease Database. (2016). *La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos*. [online] Disponible en: http://europa.eu/rapid/press-release_IP-16-2461_es.htm
- Agencia Española de Protección de datos. (2016). *Guía acerca del escudo de privacidad U.E. - EE. UU.* [online] Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Guia_acerca_del_Escudo_de_Privacidad.pdf
- Agencia Española de Protección de datos, (2018). *Guía del reglamento general de protección de datos para responsables del tratamiento*. Disponible en: www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf
- Agencia española de protección de datos. (2013). *Las Autoridades europeas de protección de datos aprueban el primer dictamen conjunto sobre aplicaciones móviles*. [online] Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/marzo/130314_NP_Dictamen_aplicaciones.pdf
- Ortega Jiménez, A. (2014). *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. [online] . Agencia Española de Protección de Datos. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/La_des_proteccion_del_titular_del_derecho.pdf