TRABAJO DE FIN DE GRADO

LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA: ASPECTOS JURÍDICOS RELEVANTES

Autora:
Clara DARNET

Directora del Trabajo:
BLANCA VILA COSTA

Trabajo de Fin de Grado

Cuarto Curso del Grado en Derecho

Facultad de Derecho

Departamento de Derecho Internacional Privado

En Bellaterra, a 11 de mayo 2017

RESUMEN

La protección de datos es el nuevo objetivo de los legisladores. De hecho, el dato tiene hoy en día la consideración de bien económico, susceptible de valoración pecuniaria, lo que tiene como consecuencia la creación de normas comunitarias a fin de proteger los usuarios europeos.
A lo largo del presente trabajo, se analizará en profundidad el nuevo reglamento de protección de datos: el Reglamento (UE) 2016/679 del Parlamento 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.

El mencionado estudio se efectúa atendiendo a los conceptos generales como peculiares de cuyo texto, así como los órganos institucionales creados por este. No se olvidará mencionar las razones de creación o desarrollo de tales normas, así como los resultados a obtener y/u obtenidos. Por consiguiente, a través del estudio de este texto europeo, se quiere entender y criticar la implicación de la protección de datos actual.

ÍNDICE

ABREVIATURAS....4

INTRODUCCIÓN....5

I. EL OBJETIVO DE LA PROTECCION 'EFECTIVA' DE LOS DATOS PERSONALES: EL CONSENTIMIENTO Y LAS TRANSFERENCIAS DE DATOS....9

A / El consentimiento claro y efectivo ante el mercado de la información ...9

1. La información como un servicio 9

2. La regulación del tratamiento para asegurar el derecho a la vida privada 13

i) El concepto de privacidad....13

ii) El establecimiento de una reglamentación....18

B / La transferencia de los datos....23

1. Cuestiones generales 23

i) Concepto de transferencias 23

ii) Una protección más amplia que en las legislaciones internas 25

2. Un reglamento adaptado a la realidad....31

II. ANALISIS PARTICULAR DE SECTORES ESPECIFICOS 33

A / 'El derecho al olvido', una mirada actualizada 34

1. Enfoque histórico 34

2. El objetivo y la reglamentación del derecho al olvido. El resultado a obtener. 38

B / El establecimiento de una protección especial para los niños 41

1. La protección de los niños como limite al tratamiento de los datos 41

2. La creación de instituciones peculiares cuyos órganos vigilan a la buena aplicación del reglamento....46

3. El resultado a obtener....50

CONCLUSIONES....51

BIBLIOGRAFIA 54

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

CE: Constitución Española de 1978

CNIL: Commission Nationale Informatique et Libertés

Directiva 95/46/CE: Directiva 95/46/CE, del Parlamento 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

Comisión: Comisión Europea

EEE: Espacio Económico Europeo

EE.UU: Estados Unidos

LOPD: Ley Orgánica 15/1999, de 14 de diciembre, de Protección de Datos de Carácter Personal

LOPJ: Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial

RGPD o Reglamento o Reglamento general de protección de datos: Reglamento (UE) 2016/679 del Parlamento 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

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

TEDH: Tribunal Europeo de Derechos Humanos

TJUE: Tribunal de Justicia de la Unión Europa

UE: Unión Europea

UNICEF: Fondo de las Naciones Unidas para la Infancia

INTRODUCCIÓN

I. Justificación de la elección del objeto estudiado

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person"[1], a través de esta cita de Warren y Brandeis, se puede destacar el objetivo principal del nuevo reglamento de protección de datos: la protección de los usuarios.

Para entender porque se debe proteger los datos, se debe primero aclarar este concepto de dato. El dato es toda información sobre una persona física identificada o identificable. Una persona puede ser identificada, directa o indirectamente, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona[2]. Por lo cual, el dato es un elemento bastante amplio, que puede reunir diversas realidades.

De hecho, el RGPD en sí nos expone los motivos de los legisladores europeos por los cuales se ha redactado este texto. Entre otros, alegan el carácter fundamental de este derecho – protegido por diversos textos internacionales – y la necesidad de adaptación a la realidad político-socio-jurídica.

Actualmente, el dato es una de las nociones fundamentales de nuestra sociedad. Esta utilizado de manera individualizada por parte de los usuarios a través de la creación de perfiles o por parte de las empresas a título económico para actuar en el mercado. De esa utilización lucrativa, nace la necesidad de crear reglas para asegurarse que las empresas no abusen de las informaciones dadas por parte de los ciudadanos.

---

[1]: Miguel Recio Gayo, *Protección de datos personales e innovación, ¿(in)compatibles?*, en Reus Editorial, Derecho de las nuevas tecnologías, 2016, p. 5

[2]: Reglamento (UE) 2016/679 del Parlamento 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 o RGPD): Articulo 4.1

De hecho, la era digital de nuestro siglo evoluciona tan rápidamente que, para asegurar una tutela efectiva de los derechos de los ciudadanos europeos, se debe ajustar esas reglas. Tras cuatro años de trabajo, el día 14 de abril de 2016 el Parlamento Europeo adoptó el Proyecto y el 27 de abril de 2016, se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo 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 ha derogado la Directiva 95/46/CE a fin de reformar la normativa ya existente para adaptarla al nuevo contexto político-socio-jurídico.

Somos consciente, con el desarrollo de los medios informáticos, del aumento de los flujos transfronterizos de datos personales[3], pero, no se debe restringir sino controlar y supervisar el tratamiento de estos. Como lo explica el reglamento estudiado, *"el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad."*[4]

Por lo que respecta a su ámbito de aplicación, conforme a su artículo 99, el Reglamento entrará en vigor "*a los veinte días de su publicación oficial en el Diario Oficial de la Unión Europea*" y "*será aplicable a partir del 25 de mayo de 2018*", momento a partir del cual "*será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro*"[5].

Este nuevo reglamento, modifica reglas ya existentes, desarrolla unas que fueron muy básicas y crea otras que ya nunca fueron recogidas en textos europeos.

[3]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Motivo 5
[4]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Motivo 4
[5]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 99

Entonces, nos aparece necesario hacer un estudio profundizado de este nuevo paquete de reglas europeas a fin de entender cómo se proteger al usuario europeo hoy en día. De hecho, la figura central de este escrito es el ciudadano europeo porque juega un papel fundamental en la nueva era digital, ya sea activo o pasivo.

II. Objetivo y metodología de investigación.

La finalidad principal de este trabajo es, analizar y reflexionar sobre el régimen propuesto a fin de asegurar una tutela efectiva de los derechos de los ciudadanos europeos, especialmente desde el punto de vista comunitario, y en particular, a través del estudio del nuevo reglamento de protección de datos del 27 de abril de 2016. Más precisamente, se trata aquí de estudiar unas cuestiones fundamentales del reglamento, ya sean novedosas o no, para examinar la protección de los residentes europeos. Para conseguir este objetivo, me propongo observar cuatro reglas.

En primera instancia, dado que el dato es un concepto amplio, estudiaremos las normativas generales y extensas propuestas por los legisladores para defender cuyo dato.

Así pues, nos centraremos en primer lugar, en el consentimiento claro y efectivo como exigencia del reglamento para asegurar el derecho a la vida privada. Analizaremos la razón de la existencia de tal consentimiento investigando el mercado de la información y esta última como servicio. Después, cabera analizar la noción de privacidad, su evolución y su impacto sobre el concepto de dato para poder entender y reflexionar sobre la legislación en vigor.

En segundo lugar, estudiaremos el otro tema central del nuevo reglamento: las transferencias de datos. Entonces, es necesario comprender el concepto de transferencias. Veremos que este concepto de transferencias esta también muy presente en las legislaciones nacionales y haremos un análisis comparativo del reglamento con las legislaciones nacionales para concluir a una mayor protección

comunitaria. Finalmente, notaremos que este texto europeo no es una simple norma actualizada, sino que se adapta a la realidad.

En segunda instancia, aunque el dato sea un concepto amplio, calificaremos una persona de única e individualizada por lo cual, será necesario, previamente, establecer normas específicas a las necesidades de cada uno.

Nos dedicaremos, primero, a investigar un sector específico, novedad de este reglamento (la Directiva 95/46/CE no la contemplaba): el derecho al olvido o derecho de supresión, de manera que, para discernir lo añadido a la reglamentación establecida, se debe estudiar su enfoque histórico. Se atenderá especialmente a la Sentencia Google de 13 de mayo de 2013. Discutiremos en siguiente cual es el resultado a obtener y si se ha alcanzado.

Para terminar, creo necesario observar la protección hacia los niños. A través de la directiva "Télévision Sans Frontière", se efectuará un análisis crítico de esa normativa especial para los menores como limite al tratamiento de los datos. Se expondrá siguientemente los órganos institucionales y reflexionaremos sobre sus papeles de tutores del reglamento. Finalmente, comprobaremos el resultado obtenido y el posible resultado que se obtendrá en un futuro próximo.

De manera sintética, podemos decir que, en este estudio, se analizará el reglamento de lo general a lo particular para poder tener una visión general y vislumbrar su lógica.

I. EL OBJETIVO DE LA PROTECCION 'EFECTVA' DE LOS DATOS PERSONALES: EL CONSENTIMIENTO Y LAS TRANSFERENCIAS DE DATOS

Se trata en primer lugar de estudiar el nuevo reglamento teniendo un punto de vista general. En efecto, ha introducido novedades de tipo global: la necesidad de un consentimiento claro y efectivo (A) y reglas y requisitos precisos sobre transferencias de datos (B).

A / El consentimiento claro y efectivo ante el mercado de la información

Este estudio tiene como objetivo el análisis de uno de los puntos fundamentales del nuevo reglamento de protección de datos, la exigencia por parte de los individuos de dar un consentimiento claro y efectivo para que se pueda emplear sus datos con fines comerciales. Sin embargo, no se puede comprender correctamente por qué se instauró este requisito, sin aclarar las razones.

1. La información como servicio

Hoy en día, la red no es uno de los medios principales sino el medio principal de búsqueda y comunicación. Por la facilidad de acceso a cualquier información requerida, se podría pensar que todo es posible, accesible y sobre todo gratis. No obstante, cuando se analiza un poco más a fondo este tema, podemos constatar que es más alambicado.

Desde siempre, la información, sea informática o no, ha sido objeto de comercio. Sin embargo, el incremento del desarrollo tecnológico e informático ha conducido a un mercado de la información. Los ciudadanos cuando usan los medios informáticos y más precisamente, la red, proporcionan datos personales que son una fuente de gran interés para la economía numérica. Estos datos tienen cierto valor pecuniario porque llevan informaciones personales que son trascendentales.

Como lo dice Bruno Lasserre, son *"un vector de dinamismo comercial"*[6]. Este carácter económico y poderoso de estos datos se desprende a la hora de explotarlos.

Cuando un ciudadano provee una información, esta última esta tratada no solamente para el propósito principal por la cual fue transmitida sino también de forma que pueda ser explotada por parte de otros operadores. Así, se puede aprovechar esa información varias veces y venderla a diversos operadores. Por lo cual, tener la información es tener el poder porque se puede controlar la transmisión de ese dato y así controlar el mercado.

En efecto, en el mercado, quien tiene el poder es quien posee la información.
Se ve por lo tanto una relación muy estrecha entre competencia y protección de datos porque *"constituye una cuestión de competencia cuando la obtención de aquellos datos personales permite a una empresa adquirir un incuestionable poder en el mercado"*[7]. Podemos tomar el ejemplo de Facebook: en función de los "likes" o "dislikes", Facebook puede establecer los gustos de cada uno de sus usuarios y vender estas informaciones a diversas empresas para que puedan enviar publicidad e incitar al consumo. Este tratamiento es legal siempre que sea leal.

Por lo tanto, se establecen estándares legales a respetar a través de normas internas, (por ejemplo, la LOPD o el Real Decreto 1720/2007[8]) pero sobre todo a través de normas europeas, reglamentos o directivas, (por ejemplo, el RGPD o la Directiva 95/46/CE[9]) que los Estados miembros deben integrar en su derecho nacional y defender.

---

[6]: Lasserre Bruno, *Le point de vue de l'autorité française de la concurrence*, en ALMUNIA, Joaquim ("et al"), New Frontiers of antitrust 2013, Competition Law in times of Economic, Bruylant, 2013

[7]: Lasserre Bruno, *Le point de vue de*, cit., para.15

[8]: Gobierno de Espana, Ministerio de Industria, Turismo y Comercio, "Normativa sobre protección de datos personas: catálogos y requisitos agrupados por materias", ISMS Forum Spain, en: http://www.protegetuinformacion.com/docs/13/lopd_PDF_tema1_proteccion_datos_personales.pdf

[9]: 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, en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al14012

Para lograr el respeto de los derechos fundamentales a través estos estándares, existen organizaciones nacionales como la CNIL en Francia o la AEPD en España. Son responsables de asegurar que la tecnología de la información está al servicio y que no afecta a los derechos humanos como la privacidad, o las libertades individuales y públicas.

Este comercio de la información es necesario. De hecho, permite promocionar productos adaptados a los consumidores y a sus gustos para satisfacerles, y atraer nuevos clientes[10]. El tratamiento de los datos es primordial para agradar a los consumidores y para extender el negocio de las empresas y así amplificar la economía porque *"la naturaleza de los datos colectados y la finalidad del tratamiento o los destinatarios de las informaciones comprendido los terceros, otorga a los consumidores medios para comparar las ofertas en función del criterio especifico de la preservación de sus datos personales"*[11].

Sin embargo, se debe destacar también que, proponiendo productos adaptados a sus gustos, se influencia al consumidor. Para entenderlo, voy a dar un ejemplo común: una persona acude a una web de ropa y selecciona un producto, pero al final no lo compra. Esta persona va luego encontrar este mismo producto en otras webs como publicidad. Así, se está haciendo un comercio con esta información, con este dato para influenciar la persona al consumo. Por lo tanto, el problema no es tan la existencia del mercado, porque como visto es necesario, sino más su utilización y aprovechamiento por parte de los operadores.

[10] : López Carballo Daniel, "Responsabilidades derivadas del tratamiento y explotación de los datos personales", 27.01.2017, en http://dlcarballo.com/2017/01/27/responsabilidades-derivadas-del-tratamiento-y-explotacion-de-los-datos-personales/

[11]: Lasserre Bruno, *Le point de vue de*, cit., para.22

De hecho, estos datos tienen tanto impacto que en paralelo al "mercado legal", existe hoy en día un mercado negro muy lucrativo como nos lo expone EfeFuture: *"El mercado del ciberdelito es muy rentable con cifras estimadas de entre 450.000 millones y el billón de dólares al año y con precios dispares por bienes o servicios que van desde un dólar por una cuenta de Facebook con quince amigos hasta 2.500 por el diseño de código malicioso comercial, según expertos"*[12].

Este mercado negro funciona de esta manera: los operadores roban las informaciones de los usuarios, *"las principales formas de robo de información están relacionadas con el phishing o malware, donde las actividades consisten en obtener datos confidenciales como contraseñas o datos financieros. Estas técnicas pretenden obtener información de las potenciales víctimas a partir de engaños y técnicas fraudulentas"*[13]. Después de haber robado las informaciones, se venden a diferentes precios según el tipo de cuenta. WeLiveSecurity ha publicado un tablón de los precios de venta en el mercado negro en función del tipo de cuenta que se piratea[14], *"como ejemplo, en el mercado clandestino se pueden comprar 1,000 cuentas de correo electrónico por precios entre 0.50 y 10 dólares"*[15]. Este mercado clandestino es tan lucrativo que todas las grandes empresas sufren de ciberataques, que sea Facebook, Linkedln, Yahoo o Twitter. Así se ve que cualquier empresa es una potencial víctima y, por consiguiente, sus usuarios también. En efecto, se pronosticó por la empresa Cisco que, en 2020 se llegará a unos 26.300 millones de dispositivos conectados lo que aumenta el riesgo de robo de informaciones y lo que incrementa también el mercado negro.

---

[12]: Quincoces Riesco Amaya, "¿Cuánto valen los datos personales en el mercado del ciberdelito?", Mercado Ciberdelito, EfeFuturo, 28.09.2015, en http://www.efefuturo.com/noticia/cuanto-valen-los-datos-personales-en-el-mercado-del-ciberdelito/

[13]: Angel Mendoza Miguel, "¿Cuánto por esa cuenta? El valor de la información en el mercado negro", WeLiveSecurity, 25.11.2016, en http://www.welivesecurity.com/la-es/2016/11/25/informacion-mercado-negro/

[14]: Angel Mendoza Miguel, "¿Cuánto por esa cuenta? El valor de la información en el mercado negro", WeLiveSecurity, 25.11.2016, en http://www.welivesecurity.com/la-es/2016/11/25/informacion-mercado-negro/

[15]: Velasco Oscar, "El costo de la información en el mercado negro", E.Security, 15.01.2015, en http://revistaesecurity.com/el-co/

Por la existencia de este mercado clandestino y el respeto no siempre automático de las normas internas por parte de los operadores, se ha decidido redactar este reglamento general de protección de datos con el fin de intentar proteger de manera más eficiente la intimidad y privacidad de los ciudadanos europeos. De hecho, *"es importante priorizar por parte de las empresas la protección de sus datos, ya que éstos se están convirtiendo en el activo más cotizado y en el petróleo del siglo XXI"*[16]. A través de este RGPD, se crean mayores estándares de protección a las empresas y sanciones como herramientas a disposición de los individuos para que tengan un mayor control sobre sus datos y su transferencia.

2. La regulación del tratamiento para asegurar el derecho a la vida privada

Con la redacción del RGPD, se da un mayor poder a los usuarios a la hora de explotar sus datos, se establece especialmente un derecho a ser informado y dar su consentimiento para el tratamiento de sus datos. Tal legislación responde a la urgente necesidad de proteger la vida privada de los ciudadanos europeos.

i) El concepto de privacidad

La palabra privado proviene del latín "privatus" y del correspondiente verbo "privare" que significa privar. La privacidad se puede definir como aquello que lleva a cabo una persona fuera del ámbito público, en un ámbito reservado.
El derecho a la privacidad es un derecho fundamental recogido en la Declaración Universal de los Derechos Humanos (articulo 12). Este derecho está vinculado con el derecho a la intimidad: *"zona abstracta que una persona reserva para un grupo acotado de gente, generalmente su familia y amigos. Sus límites no son precisos y dependen de distintas circunstancias"*[17].

[16]: De La Higuera Ana, "El mercado negro de la información y el nuevo Reglamento de Protección de Datos", KPMG Blogs, 22.11.2016, en http://www.kpmgblogs.es/el-mercado-negro-de-la-informacion-y-el-nuevo-reglamento-de-proteccion-de-datos/
[17]: Pérez Porto Julián y Merino María, Definición de la intimidad, 2014, en http://definicion.de/intimidad/

Estos dos derechos, están también protegidos por las Constituciones de cada país: en España es protegido por los artículos 17 y 18 *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*[18] o también en Francia por el articulo 2 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789 y el artículo 9 del Código Civil. Al nivel europeo, está protegido por el Convenio 108 del Consejo de Europa.

Sucede que la vida personal de una persona se desarrolla dentro de un espacio reservado y este último debe mantenerse en la intimidad. Este ámbito privado recoge varios componentes, como, por ejemplo, la vida íntima, preferencias políticas, religión, datos personales, correos, datos sobre la salud, comunicaciones privadas etc.

Este concepto de vida privada es muy importante porque desde la Antigua Grecia, ha sido objeto de controversias. En efecto, en esta época, las cuestiones sociales, políticas o económicas de la 'polis' se llevaban a cabo en el ágora. Se celebraban asambleas para discutir sobre la vida de la nación. Así, el ámbito privado de cada persona era bastante restringido. El concepto de privacidad ha evolucionado a través de los siglos. Tal como lo señala en su tesis, Emilia Zaballos Pulido, *"el origen del concepto jurídico de intimidad es anglosajón y en concreto procede del derecho norteamericano."*[19]

Nos indica que el artículo de Samuel Warren y Louis Brandeis publicado en 1890 en la Harvard Law Review titulado "The Right to Privacy", conceptualiza el derecho a la privacidad. A partir de ese momento, las potencias democráticas mundiales empezaron a desarrollar ese concepto en sus ordenamientos internos.

[18]: Articulo 18 de la Constitución Española, "Derecho al honor, a la intimidad y a la propia imagen", en http://noticias.juridicas.com/base_datos/Admin/constitucion.html
[19]: Zaballos Pulido Emilia, Tesis doctoral, en http://eprints.ucm.es/22849/1/T34733.pdf

Utilizando la clasificación generacional[20], son considerados como derechos de primera generación: los derechos civiles y políticos. *"Están vinculados al principio de libertad y su característica fundamental viene determinada porque exigen de los poderes públicos su inhibición y no injerencia en la esfera privada. La primera generación surge con el Bill of Rights de los nuevos EEUU y la Declaración de los Derechos del Hombre y el Ciudadano de la Revolución francesa"*[21].

Estas características explican la creación del nuevo paquete de protección de datos. En efecto, los datos forman parte del ámbito privado – el derecho a la privacidad es un derecho de primera generación – ámbito intensivamente protegido nacional e internacionalmente y sería un aberrante que no existiera una protección europea.

Con el desarrollo exaltado de la era digital, el concepto tradicional posee una nueva conceptualización autónoma. A día de hoy, se ha demostrado que la protección de datos es un derecho fundamental porque deriva del derecho a la privacidad. Fue exhibido entre otros por la sentencia Lindqvist de 2003 del Tribunal Europeo[22].

Con este cambio dactilar, nos podemos preguntar si realmente tenemos privacidad o si es solo una utopía. La brecha que separa el privado del público es cada más fina, como lo ponen de relieve estas cifras: "*Para los usuarios franceses, lo que más les gusta de Internet es la herramienta de comunicación facilitadora (61%), organizar y gestionar la vida diaria (36% de los internautas) creciendo (35%), jugar y divertirse (23%) y aprender acerca de noticias nacionales (21%)"*[23].

---

[20]: La clasificación generacional fue creada en 1979 por primera vez por el profesor y miembro del Instituto de Derechos Humanos de Estrasburgo, Karel Vasak. "Este autor consideraba que en la evolución histórica de los Derechos Humanos pueden distinguirse tres generaciones, asocia- da cada una de ellas al desarrollo de los tres grandes valores proclamados en la Revolución Francesa: Libertad, Igualdad y Fraternidad".
Fraguas Madurga Lourdes, "El concepto de derechos fundamentales y las generaciones de derechos", *Anuario del Centro de la Universidad Nacional de Educación a Distancia en Calatayud. N.o 21*, pp. 117-136, 2015, *en* http://www.calatayud.uned.es/web/actividades/revista-anales/21/03-05-LourdesFraguasMadurga.pdf

[21]: Fraguas Madurga Lourdes, "El concepto de derechos fundamentales y las generaciones de derechos", *Anuario del Centro de la Universidad Nacional de Educación a Distancia en Calatayud. N.o 21*, pp. 117-136, 2015, en http://www.calatayud.uned.es/web/actividades/revista-anales/21/03-05-LourdesFraguasMadurga.pdf

[22]: STJUE Caso C-101/01, Bodil LindqvistL, de 6 de noviembre de 2003, en : http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d6b3e72d7f664a440d9956b8b3324e9058.e34KaxiLc3eQc40LaxqMbN4Pax0Ke0?text=&docid=48382&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=30433

[23]: "Les usages variés du Net", IAB France, en http://www.iabfrance.com/contenu/dossiers/fiches/les-usages-varies-du-net

Así, en lugar de tener una ubicación geográfica y física como el ágora de la Antigua Grecia, tenemos un lugar ilimitado y no totalmente entendido. De hecho, los usuarios pueden guardar sus carpetas, documentos, archivos, fotos en espacio de almacenamiento llamados 'Cloud', *"la idea de cloud computing (informática en nube) –inspirada en una arquitectura cuyo estado natural consiste en una pila de recursos fuera de la empresa, proporcionados por un proveedor externo, y soportados y compartidos a través de Internet"*[24]. Por lo cual, este Cloud parece muy útil: permite un acceso a sus datos desde cualquier lugar del mundo siempre y cuando tenga una conexión internet y la preservación de los datos para no perderlos si un problema informático ocurre. Sin embargo, como dije, los ciudadanos e incluso los informáticos no saben realmente donde se almacenan esas copias. De hecho, la ventaja principal es poder acceder a sus documentos desde cualquier lugar del mundo; pero si los usuarios pueden acceder esto significa que los piratas también pueden hacerlo. Así, al robar una contraseña, se pueden robar documentos que están bajo la privacidad del usuario.

Con el aumento de los flujos transfronterizados y la existencia de un mercado negro, la información actualmente es puro oro para los piratas. Asistimos a un cambio radical del concepto de la vida privada que desemboca en un enfrentamiento entre la privacidad y la democratización de internet. Debemos, como juristas, encontrar un equilibrio con el fin de preservar la privacidad de los ciudadanos asegurando al mismo tiempo el avance tecnológico. Ese equilibrio se encuentra en una protección efectiva de los datos de los usuarios.

Las empresas son conscientes de este fenómeno y se sienten concernidas. En este sentido, podemos hablar de la decisión de Microsoft al respeto del 'Privacy Shield', *"Microsoft was proud to become the first global cloud service provider to appear on the Department of Commerce's list of Privacy Shield certified entities as of August 12th 2016. The European Commission adopted The EU-US Privacy*

[24]: "Los peligros del modelo cloud computing", CSO Digital, ComputerWorld, 22.09.2008, en http://cso.computerworld.es/cloud/los-peligros-del-modelo-cloud-computing

Shield Framework on July 12th 2016, replacing the International Safe Harbor Privacy Principles as the mechanism for allowing companies in the EU and the US to transfer personal data across the Atlantic in a manner compliant with the EU data protection requirements"[25]. Por este acuerdo, Microsoft, empresa de grande dimensión, manifiesta su aprobación al respeto de las decisiones tomadas en la Unión Europea y se ve preocupada por la privacidad de sus usuarios y por la plena aplicación del RGPD, especialmente en tema de transferencia de datos, lo que estudiaremos luego.

Con el avance tecnológico, es imprescindible adaptar las legislaciones para proteger la privacidad de los ciudadanos y garantizar una tutela efectiva. El órgano encargado de hacer respetar estas normas europeas es el TJUE, con el apoyo de la TEDH. En efecto, posteriormente a la entrada en vigor del reglamento, el TJUE ha dictado diversas sentencias en las cuales se ve claramente que quiere empezar la aplicación del reglamento de manera progresiva. En lo que concierne la privacidad, podemos alegar la sentencia del 21 de diciembre de 2016 (asunto conjunto C-203/15 y C-698/15) en el cual *"el Derecho de la Unión se opone a una "retención generalizada e indiscriminada" de los datos de tráfico y de localización [∴] y observa, en particular, en lo que respecta a la conservación, que conserva los datos tomados en conjunto pueden ser capaces de sacar conclusiones muy precisas acerca de la privacidad de las personas cuyos datos se han almacenado"*[26]. El hecho de que la retención de datos se lleva a cabo sin que los usuarios de servicios de comunicaciones electrónicas lo sepan, puede generar en la mente de los interesados, la sensación de que se está supervisando su privacidad constantemente.

---

[25]: Rison Alice, "Microsoft Cloud is first CSP behind the Privacy Shield", Microsoft Azure, 26.09.2016, en https://azure.microsoft.com/en-us/blog/microsoft-cloud-is-first-csp-behind-the-privacy-shield/

[26]: STJUE Asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department, de 21 de diciembre de 2016, en, http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=ES

Por lo tanto, sólo la lucha contra la delincuencia grave puede justificar tal interferencia[27].

Podemos también exponer la sentencia de la TEDH Vukota-Bojić c. Suisse (asunto 61838/10) del 18 de octubre de 2016 en el cual se decidió que la supervisión de una víctima de accidente de la carretera por una compañía de seguros era ilegal porque violó su derecho a la privacidad[28].

Por lo tanto, en lo que concierne los datos personales, como son elementos de la privacidad de cada persona, vemos que existe una estrecha conexión entre el TJUE y la TEDH. Esta conexión tiene como objetivo certificar la defensa de la privacidad de los ciudadanos europeos.

ii) El establecimiento de una reglamentación

En las redes sociales como Facebook, Twitter y Tuenti, los problemas más importantes que estos servicios generan al derecho fundamental son la publicación excesiva de información personal, bien sea información propia o de terceras personas. Esto es una de las razones por las cuales el RGPD ha establecido nuevas normas y reglas de protección de los datos. Una de las más relevante es el derecho a ser informado (articulo 7) y dar un consentimiento claro y afirmativo a la hora de tratar los datos (artículos 5, 6, 7, 8, 11, 12 y el capítulo IV).

En su artículo 4, el RGPD provee diversas definiciones y especialmente la del tratamiento y del consentimiento del interesado. El tratamiento se define como *''cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación*

---

[27]: "Dans un arrêt, la CJUE estime que les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications électroniques", Droits fondamentaux, lutte contre la discrimination - Justice, liberté, sécurité et immigration, EuropaForum, 21.12.2016, en http://www.europaforum.public.lu/fr/actualites/2016/12/cjue-donnees/index.html

[28]: Sentencia de la TEDH Caso no 61838/10**,** Vukota-Bojić v. Switzerland, de 18 de octubre de 2016, en http://hudoc.echr.coe.int/fre#{"itemid":["001-167490"]}

por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"[29] y el consentimiento del interesado como *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*[30].

De estas dos definiciones, se deduce que no basta con el simple consentimiento tácito, puesto que es necesario 'una declaración o una clara acción afirmativa'.
El legislador, con estas definiciones precisas y este requisito de consentimiento expreso, se asegura que el usuario ha entendido claramente cómo y en qué contexto se están tratando sus datos. En este sentido, los operadores a la hora de recoger la información para tratarla, deben definir de manera clara y comprensible las cláusulas de privacidad. En efecto, *"se exige mayor claridad en las cláusulas informativas de los servicios digitales y en las políticas de privacidad, en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento"*[31].

Así, se refuerza el control de los usuarios sobre sus datos, dado que, en las leyes internas, como la LOPJ en España, un solo consentimiento tácito era suficiente.
Con la aplicación del nuevo reglamento, además de obtener este consentimiento, los operadores deben registrarlo a fin de probar que lo han recibido.

Esta necesidad de consentimiento viene de la necesidad de autonomía contractual en el derecho de los contratos. Cuando dos partes establecen un acto jurídico, aquel que se compromete, debe haber dado su consentimiento.

---

[29]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 4.2
[30]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 4.11
[31]: Brocca Marina, "El nuevo reglamento de protección de datos", Protección de datos, 20.10.2016, en https://marinabrocca.com/proteccion-de-datos/nuevo-reglamento-proteccion-datos/

Incluso cuando el contrato es una obligación legal, siempre se requiere el consentimiento, a pesar de que uno podría pensar que la ley puede sustituir consentimiento. No hay nada, y los casos en los que el consentimiento no es posible son muy raros y motivados por razones de orden público.

Además, existe contrato una vez que el consentimiento es dado sobre los elementos esenciales. Por lo cual, si la persona no ha concedido su consentimiento sobre los elementos accesorios, todavía el contrato se tiene por perfección.
Este consentimiento se manifiesta por la aceptación de los términos y debe ser puro y simple, es decir que se tiene que aceptar la proposición de la otra parte, si se modifica alguna parte, no es aceptación sino contra-proposición.
En lo que concierne las nuevas contrataciones por electrónico, se ha creado el sistema del "doble clic": el primer clic permite verificar el orden y el segundo aceptar y manifestar su consentimiento.
Aunque el consentimiento sea necesario, se puede preguntar sobre su realidad. De hecho, se pide consentimiento al ciudadano, pero si él no le da, no podrá acceder a la información. Hoy en día, no se trata solamente de contratos típicos como el de compraventa sino también de contratos de 'información' en los cuales para acceder a la información se debe prestar consentimiento. Por lo cual, hoy en día se pide todavía ese consentimiento, pero el ciudadano no es libre, el consentimiento es parecido a un requisito para poder llegar a la información.

Además, en lo que concierne el tratamiento de los datos, una vez que los operadores han adquirido el consentimiento, éste debe hacerse con licitud. Quiere decir que el tratamiento debe ser licito y leal. Esta obligación de tratamiento leal la encontramos al artículo 5 del RGPD "*los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)"*[32] pero también en las legislaciones internas como en los artículos 4 y 8 de la LOPD *"los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento,*

[32]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 5

cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"[33]. Conjuntamente con estos principios de transparencia, consentimiento expreso y trato leal, encontramos el principio de información. Eso quiere decir que el usuario tiene el derecho a ser informado cuando se utilizan sus datos. Así entre otros, se debe advertir a las personas cuando los datos personales se están recogiendo, utilizando o consultando, los fines del tratamiento, a qué se destinan los datos personales y la base jurídica del tratamiento, la identidad de los destinatarios o las categorías de destinatarios de los datos personales, la identidad del responsable de la gestión y si procede, del delegado de protección de datos o también la existencia del derecho a solicitar al responsable del tratamiento el acceso[34]. Finalmente, este derecho de información procede también cuando los datos han sido pirateados (novedad del reglamento).

Este RGPD pretende además unificar las reglas aplicables en tema de protección de datos como destacado en la sentencia Amazon, asunto C521/11[35]. En efecto, cuando será de plena aplicación, este reglamento vendrá derogar a todas las normas ya establecidas. Se crea una sola norma aplicable con el fin de uniformar para garantizar una tutela efectiva. En efecto, si una sola norma está vigente, no podrán surgir problemas de aplicación de directivas o reglamentos, saber cuál aplicar y cuando. Con una sola norma, se resuelven estos tipos de problemas que pueden surgir. Como lo dice Jan Albrecht (Verdes, Alemania), responsable de la tramitación parlamentaria del texto, *"Con este reglamento de protección de datos conseguimos un nivel uniforme de protección en toda la UE.*

[33]: Agencia Española de Protección de Datos, "Principios relativos a la calidad de los datos", Calidad de datos, en https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/calidad_de_datos/index-ides-idphp.php

[34]: Brocca Marina, "El nuevo reglamento de protección de datos", Protección de datos, 20.10.2016, en https://marinabrocca.com/proteccion-de-datos/nuevo-reglamento-proteccion-datos/

[35]: STJUE, Caso C-521/11, Amazon, de 11 de julio de 2013, en http://curia.europa.eu/juris/document/document.jsf?text=&docid=139407&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=109092

Es un gran éxito para el Parlamento y un 'sí' claro a los derechos de los consumidores y a la competencia en la era digital. Los ciudadanos podrán decidir por sí mismos qué información quieren compartir"[36].

Por fin, se debe aclarar un último punto. Existen unos límites al derecho a la vida privada que son el interés legítimo o interés público. Como lo sabemos, en un Estado de derecho, el interés general prima sobre los intereses singulares. Así, por causa de interés público y con un control de proporcionalidad, se podrá limitar el derecho a la vida privada. Esa noción de interés público no es definida por el reglamento, pero, sí que encontramos a su artículo 23 las limitaciones a la protección de los derechos protegidos por el RGPD; entre otros se alega la defensa o la seguridad pública [37]. Esas limitaciones pueden, por lo tanto, ser aplicadas por interés público puesto que las nociones de interés público y limitación están muy vinculadas.

Sin embargo, se puede ver que todas estas limitaciones del articulo 23 se remiten a las jurisdicciones internas. En efecto, si tomamos el ejemplo de la seguridad pública, cada Estado deberá hacer una valoración proporcionada, pero es inherente a cada Estado de decidir cuándo se puede limitar por causa de seguridad pública. No existen estándares fijos europeos, es a la apreciación de cada Estado y en consecuencia esta noción puede ser peligrosa por su amplitud y por el hecho de que puede abarcar un cúmulo de situaciones.

[36]: "Las nuevas normas de protección de datos aprobadas por el Parlamento Europeo devuelven su control a los ciudadanos", ConfiLegal, 14.04.2016, en https://confilegal.com/20160414-las-nuevas-normas-proteccion-datos-devuelven-control-los-ciudadanos/

[37]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 23

B / La transferencia de los datos

Una vez que los operadores han recogido el consentimiento de los usuarios, pueden transferir los datos fuera de Europa, pero respetando reglas específicas. Por eso, es necesario estudiar otra innovación fundamental general: la regulación de las transferencias de datos. Es de considerable importancia el estudio de la regulación de las transferencias en el RGPD porque hubo grandes modificaciones en relación a las legislaciones internas.

1. Cuestiones generales

Estados Unidos, siendo una de las potencias económicas más importantes del mundo, nos aparece claramente unas relaciones no insignificantes. Con la abolición del acuerdo *Safe Habour*[38], la Comisión europea debía instaurar un régimen de protección de las transferencias de datos de sus ciudadanos. Por lo cual, cuando se redactó el nuevo reglamento sobre protección de datos, incluyo un capítulo sobre transferencias de datos, capítulo aplicable no solamente a Estados Unidos sino también a todos los Estados terceros. Así pues, no solamente ha establecido un régimen limitativo y rígido, sino que ha también precisado el concepto de transferencias de datos.

i) Concepto de transferencias

Aunque la regulación de las transferencias de los datos sea tratada en un capítulo entero del reglamento, carece de definición comunitaria. Por lo cual, se debe ir a las legislaciones internas de cada país para tener una definición. En España, se regula en los artículos 33 y 34 de la LOPD y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, (RLOPD).

[38]: El Safe Harbor era un conjunto de principio negociados entre Estados Unidos y la UE, para obtener la autorización para transferir los datos personales a efectos del EEE a los EE.UU.

En un nivel interno se podría decir que un tratamiento de datos supone una transmisión fuera del territorio español pero desde que se constituyó el Espacio Económico Europeo y dado el nivel de protección uniforme sobre cuyo territorio, se puede definir como *"transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"*[39]. De una manera sintética, se puede decir que el tráfico internacional de datos personales es la transmisión de los datos, desde un ordenamiento inicial (en nuestro caso, los Estados miembros de la Unión), hacia un destinatario establecido en un territorio extranjero[40].

A este efecto, se puede adicionar que el Tribunal de Justicia de la Unión Europea ha precisado ese concepto de transferencias en su sentencia "Lindqvist", de 6 de noviembre de 2003 (Asunto C-101/01-Bodil Lindqvist). El TJUE debía determinar si la difusión de datos personales en una página web, de modo que dichos datos resulten accesibles a cualquier persona que se conecte a Internet constituían o no una transferencia internacional de datos en sentido del artículo 25 de la Directiva 95/46/CE[41]. El Tribunal respondió que *"no existe una transferencia a un país tercero de datos en el sentido del articulo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio Internet en el que se puede consultar la página web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros".*[42]

[39]: AEPD, "Cuestiones sobre cumplimiento del apartado de transferencias internacionales", en https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_cumplimiento/index-ides-idphp.php

[40]: Sancho Villa Diana, *Transferencia internacional*, ob. cit., p. 25 y 26.

[41]: AEPD, "Cuestiones sobre cumplimiento del apartado de transferencias internacionales", en https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_cumplimiento/index-ides-idphp.php

[42]: STJUE Caso C-101/01, Bodil LindqvistL, de 6 de noviembre de 2003, para. 71, en : http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d6b3e72d7f664a440d9956b8b3324e9058.e34KaxiLc3eQc40LaxqMbN4Pax0Ke0?text=&docid=48382&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=30433

En efecto, el Tribunal argumenta su posición diciendo que para que haya transferencia de datos, debe existir una relación "directa" entre dos personas. El hecho de que cualquier persona pueda acceder a la información desde un tercer país no implica una transferencia en sí: *"el concepto de «transferencia» implica que una persona situada en un lugar determinado transmite un dato a una tercera persona situada en otro lugar"*[43].

Así, en una transmisión de datos tenemos dos personas, el exportador[44] (persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero) y el destinatario[45] (la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comunican datos personales, se trate o no de un tercero). Se debe señalar que un cambio mayor introducido por el RGPD en relación con la Directiva 95/46/CE es la definición de destinatario. En efecto, la Comisión Europea manifiesta su deseo de ser más extensiva y efectiva en su protección porque ha decidido que entraran como destinatarios tanto los países terceros y organizaciones internacionales como un territorio o uno o varios sectores específicos de ese tercer país.

ii) Una protección más amplia que en las legislaciones internas

Con la creación del EEE se establecieron normas mínimas a respetar entre Estados miembros de este espacio. Sin embargo, los legisladores europeos, para proporcionar una protección efectiva, tenían que regular también las relaciones con países terceros.

---

[43]: STJUE Caso C-101/01, Bodil LindqvistL, de 6 de noviembre de 2003, para. 55, en : http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d6b3e72d7f664a440d9956b8b3324e9058.e34KaxiLc3eQc40LaxqMbN4Pax0Ke0?text=&docid=48382&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=30433

[44]: AEPD, "Transferencias internacionales de datos", en https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

[45]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 4.9

En efecto, cuando se trata de relaciones entre Estados miembros de la Unión, como cada uno debe respetar estándares de protección por pertenecer a la Unión, se puede considerar que se logra la tutela efectiva. Sin embargo, cuando se trata de intercambios con países terceros, estos no tienen que respetar normas europeas.

De hecho, no se puede permitir que una vez que los usuarios han dado su consentimiento, se puedan usar de sus datos con total libertad (como lo vimos, la competencia y los datos personales tienen una relación muy estrecha, puesto que una regulación es necesaria para garantizar la privacidad). Por eso, se han establecido los derechos ARCO[46]. En España, esos derechos son protegidos por la AEPD. Son los derechos de información, acceso, rectificación, cancelación y oposición que puede ejercer en cualquier momento un ciudadano en relación con sus datos. Así, en las transferencias de datos, el factor clave es la evaluación del nivel de protección que ofrece el país destinatario[47].

A fin de garantizar una protección real y adecuada al mundo digital en el cual vivimos, la Comisión establece un sistema de 'nivel adecuado' de protección. El reglamento habla de *"transferencias basadas en una decisión de adecuación".* Para evaluar que un país tenga un adecuado nivel de protección, la Comisión se basa en diferentes criterios como[48]:

- la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos

[46]: AEPD "Principales derechos", en http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php

[47]: Cazurro Barahona Víctor, "Transferencias internacionales de datos", en http://www.aranzadi.es/sites/aranzadi.es/files/creatividad/Publicaciones/email_pracitucm_proteccion_datos_2016/images/CapituloPracticumPDatos2015.pdf

[48]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 45.2

- los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.
- el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluída la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluídas las normas sobre transferencias ulteriores de datos personales.

Se añade también en el reglamento unas precisiones sobre la validez de comunicaciones a la vista del derecho de la Unión. En efecto, el articulo 48 nos dice que *"Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua"*[49]. Por lo cual, extiende las posibilidades de transferencias: serán aceptables las basadas en una sentencia de un tribunal o decisión de una autoridad administrativa, pero siempre obedeciendo a unas garantías; que esta sentencia o decisión se base en un acuerdo internacional entre la Unión y el tercer país.

Después del estudio, la Comisión, vía un acto de ejecución declara que el país tercero o la organización tiene un nivel adecuado de protección. Este acto de ejecución es muy importante porque permite que la transferencia se haga sin ninguna autorización.

[49]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 48

Eso quiere decir que una vez que el tercer país o la organización internacional es declarada con un nivel suficiente de protección, se puede hacer transferencia y este país u organización podrá tratar los datos sin ninguna autorización requerida por parte de la Comisión. Estos actos de ejecución son a continuación publicados en el Diario Oficial de la UE y en su página web.

En el otorgamiento de actos de ejecución, la Comisión hace un trabajo complementario con los Estados miembros. En efecto, de acuerdo con el articulo 46.5 del RGPD, *"Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo"*[50]. Esto quiere decir que hasta que sean declaradas inválidas o que sean modificadas, las autorizaciones otorgadas por los Estados miembros o la Comisión en virtud de la Directiva 95/46/CE (derogada por la nueva legislación) permanecen válidas.

Siguiendo esta misma idea de cooperación, el reglamento establece a su artículo 50 un sistema de cooperación entre la UE y los países terceros y organizaciones a fin de crear y promover mecanismos para la protección de los datos personales. Entre otros podemos citar una mutua asistencia al nivel internacional en cuánto a la aplicación de la legislación como crear fórum de debates y discusiones.

Sin embargo, se debe destacar que un solo acto de ejecución no será siempre válido. En efecto, se ha establecido un mecanismo de revisión periódico al menos cada 4 años para asegurarse que el país u organización sigue teniendo una adecuada política de protección.

[50]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 46.5

Esta revisión tendrá en cuenta todos los acontecimientos relevantes durante los 4 años anteriores[51]. Además, el reglamento ha implantado un sistema de garantías que completa el acto de ejecución y el sistema de revisión del mismo. De hecho, el tercer país u organización debe ofrecer garantías adecuadas y acciones legales efectivas a los ciudadanos para que se pueda transmitir los datos.

Por fin, a efectos de reforzar la protección y asegurar a los ciudadanos una protección total, se ha instaurado que en cualquier momento si se demuestra que *"un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo"*[52]. Esto quiere decir que, en cualquier instante, la Comisión puede decidir retirar al país u organización su calificativo de 'nivel adecuado de protección' cuando tiene una prueba relevante.

De esta manera, podemos ver el deseo de los legisladores europeos de establecer una norma protectora para sus ciudadanos. Esta aspiración se ve tanto en la amplia definición dada por el reglamento como por la existencia de formalidades muy exigentes para poder estar considerado como tercer país u organización con 'nivel adecuado de protección'. Esta nueva regulación establece mecanismos más protectores que las legislaciones internas de los Estados miembros, especialmente en tema de transferencias. Se puede pensar que quieren hacer frente a los grandes operadores tipo Google o Yahoo!.

[51]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 45.3
[52]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 45.5

En efecto, en lo que concierne este último, recientemente, sufrió de un robo masivo de datos personales de mil millones de cuenta de usuarios. *"Yahoo explica en su nota de prensa que 'una tercera parte no autorizada' accedió a los datos de sus usuarios"*[53]. Reforzando este sistema de transferencias a terceros, se puede esperar que este tipo de conducta no será posible en el futuro.

Posibles transferencias a Estados u organizaciones terceras

Sistema 1: Evaluación por la Comisión del 'nivel adecuado' de protección.

Requisitos:

- Existencia de autoridades de control independientes
- Existencia de compromisos internacionales del tercer país en relación con protección de datos
- Existencia de un Estado de derecho y respeto de los derechos humanos y libertades fundamentales

Si cumplimiento de los requisitos

Otorgamiento de un **acto de ejecución**:

- Por parte de la Comisión
- Por parte de los Estados Miembros en virtud de la Directiva 95/46/CE

Publicación del acto en el DOUE + página web

Transferencia posible **sin autorización**

Revisión del acto de ejecución cada 4 años y sistema de garantía del respeto de los derechos

- en caso de prueba relevante, la Comisión puede retirar en cualquier momento el acto de ejecución al tercer país.

[53]: Pozzi Sandro, "Yahoo anuncia el robo de datos de mil millones de cuentas », El Pais, 15.12.2016, en http://tecnologia.elpais.com/tecnologia/2016/12/14/actualidad/1481753868_540005.html

Sistema 2: Transferencia posible gracias a una sentencia de un tribunal o decisión de una autoridad administrativa basada en un acuerdo internacional entre la UE y el tercer país.

2. Un reglamento adaptado a la realidad

Como juristas sabemos que generalmente cuando se establece una regla general, viene acompañada por una excepción. El reglamento no es inmune a este precepto.

Al artículo 49 del mismo, se establecen unas excepciones en situaciones específicas. Así, en ciertas situaciones, se podrá realizar una transferencia, aunque el país tercer u la organización no tenga el acto de ejecución comprobante de su suficiente seguridad. No es necesario acreditar de un acto de ejecución por parte del tercer país u organización únicamente si se cumple una de las siguientes condiciones[54]:

- el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas
- la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado
- la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
- la transferencia sea necesaria por razones importantes de interés público
- la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones

[54]: Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 49

- la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento
- la transferencia se realice desde un registro público que tenga por objeto facilitar información al público, y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta

Sin embargo, aquí la Comisión europea no ha creado estas excepciones. En efecto, la mayoría existían en las leyes nacionales. A título de ejemplo, en España, les podemos encontrar al artículo 34 LOPD. Por lo cual, el papel de la Comisión solo fue de armonizar estas excepciones para todos sus miembros.

Además, esta nueva regulación incluye una directiva sobre transmisión de datos para cuestiones judiciales y policiales. Se aplicará al intercambio de datos transfronterizos dentro de la UE y establecerá estándares mínimos para el tratamiento de datos en cada país. La intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales, sea como víctimas, acusados o testigos, mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. Se han incluido salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación más rápida y efectiva entre las autoridades policiales y judiciales. *"El principal problema ante los ataques terroristas y otros crímenes trasnacionales es que los cuerpos judiciales y de seguridad son reacios a compartir información valiosa"*, explicó la ponente de la directiva, Marju Lauristin (S&D, Estonia).

"Al fijar estándares europeos para el intercambio de información, esta norma se convertirá en una herramienta útil para ayudar a las autoridades a trasladar datos personales

de manera sencilla y efectiva, asegurando el respeto al derecho fundamental a la privacidad", agregó[55].

Por lo tanto, en tema de investigaciones judiciales y policiales, el reglamento queda derogado por esa directiva, cuya se aplica dentro del ordenamiento europeo. Podemos decir que las transferencias de datos son un tema muy sensible – se debe en cualquier caso proteger los datos de los ciudadanos y aun en la Unión se establecen todavía estándares mínimos de protección – sobre el cual la Comisión tiene que velar cada día.

Se debe añadir que, siendo una directiva, debe ser transpuesta en el ordenamiento jurídico interno. Los países tienen un plazo de 2 años para hacerlo. El hecho de que sea una directiva y no un reglamento muestra que, aunque la Comisión quiere establecer estándares mínimos, está consciente que en algunos temas – judiciales y policiales – los diferentes sistemas comunitarios no permiten una aplicación rígida. Para que la protección sea efectiva, se la debe adaptar en cada ordenamiento jurídico según los sistemas propios (pero siempre respetando el núcleo establecido).

II. ANALISIS PARTICULAR DE SECTORES ESPECIFICOS

Ahora que hemos estudiado la parte general del nuevo reglamento, nos toca estudiar las innovaciones específicas. Nos centraremos en dos puntos: el derecho al olvido tras la sentencia Google[56] (A) y la creación de una protección especial para los niños (B).

Me parece muy importante estudiar estos conceptos, dado que forman parte de la vida cotidiana de cada uno.

---

[55]: "Las nuevas normas de protección de datos aprobadas por el Parlamento Europeo devuelven su control a los ciudadanos", ConfiLegal, 14.04.2016, en: https://confilegal.com/20160414-las-nuevas-normas-proteccion-datos-devuelven-control-los-ciudadanos/

[56]: STJUE Caso C-131/12 Google Spain, S.L, Google Inc. Vs Agencia Española de protección de datos y Mario Costeja Gonzalez, en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

De hecho, en lo que concierne el derecho al olvido o derecho de supresión, cuando un usuario quiere suprimir un perfil suyo, nos podemos preguntar lo que hace el operador con los datos proveídos: ¿se les guarda o debe suprimirlos? En efecto, algunos ciudadanos crean perfiles, pero puesto que todo evoluciona muy rápidamente, acaban siendo perfiles solo temporales que se quiere suprimir. Por lo cual, se puede plantear esta pregunta.

Por otro lado, en lo que concierne los niños, han nacido con la era digital así que todo es muy evidente e innato para ellos. Sin embargo, no son conscientes de los posibles riesgos que pueden ocurrir. Siendo la nueva generación y no lucido en cuento al peligro, se les debe proteger. Para lograr estos propósitos, se debe establecer unas reglas específicas, limitativas y salvaguardadas de sus informaciones. Por lo tanto, se debe analizar qué protección se proporciona para los menores.

A / 'El derecho al olvido', una mirada actualizada

El derecho al olvido es una de las novedades del nuevo reglamento. En efecto, tal derecho no era presente en la Directiva 95/46/CE.
Para entender por qué los legisladores han decidido integrarlo en el RGPD, nos corresponde el estudio histórico de tal derecho para después poder entender su regulación europea.

1. Enfoque histórico

Aunque el derecho al olvido sea bastante nuevo y consagrado en este nuevo reglamento, para encontrar una definición, se debe ir a la AEPD. Por lo cual, es *"la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. Hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de 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."[57]

Se puede decir que este derecho es parecido a un derecho de supresión. En efecto, la AEPD nos habla de 'derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta', pero en la red, es muy difícil sino casi imposible de limitar la difusión de información. Así uno de los medios para alcanzar este objetivo es muy radical: la supresión de la información. Por lo cual, se puede decir que el derecho al olvido es muy parecido a un derecho de supresión y/o cancelación.

El derecho al olvido en las instituciones europeas surgió con las primeras declaraciones públicas de Viviane Reding cuando dijo que *"los usuarios de Internet deben tener un control efectivo sobre lo que suben online y ser capaces de corregir, retirar y suprimirlo. Necesitamos aproximarnos a la idea del reconocimiento de un "derecho al olvido"*.[58]

Sin embargo, con estas primeras declaraciones, se confundió el derecho al olvido y la portabilidad de los datos. En efecto, en estos momentos, la mudanza de las cuentas y perfiles de unas plataformas a otras o la imposibilidad de destruirlas eran problemas vinculados[59].

Así, se puede explicar la Comunicación de la Comisión Europea de 4 de noviembre de 2010[60] sobre 'Un enfoque global de la protección de datos personales en la Unión Europea'.

---

[57]: AEPD, "Derecho al olvido", en http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

[58]: Rallo Artemi, *El derecho al olvido en Internet, Google versus España*, Centro de Estudio Políticos y Constitucionales, Madrid, 2014, p. 35

[59]: Rallo Artemi, *El derecho al olvido en Internet, Google versus España*, Centro de Estudio Políticos y Constitucionales, Madrid, 2014, p. 36

[60]: Comunicación de la Comisión Europea de 4 de noviembre de 2010 sobre "un enfoque global de la protección de datos personales en la Unión Europea: el olvido como 'cancelación' de datos personales, en http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009

En tal comunicación, la Comisión propone ejes para reforzar y lograr el control sobre los datos personales[61]:

- Reforzar el principio de la minimización de datos
- Mejorar las condiciones de un verdadero ejercicio de los derechos de acceso, rectificación, supresión y bloqueo
- Garantizar la portabilidad de los datos
- Clarificar el derecho al olvido como derecho de las personas a que sus datos dejaran de utilizarse y se suprimieran cuando ya no fueran necesarios

Esta necesidad de implantar el derecho al olvido responde, como lo ha remarcado Ordóñez Solís al hecho de que: "*Internet está planteando nuevos desafíos para los derechos fundamentales hasta el punto de que precisamente la informática ha propiciado el desarrollo extraordinario de un derecho fundamental consagrado recientemente por la Carta de Derechos Fundamentales de la Unión Europea: el derecho a la protección de los datos personales."*[62]

De hecho, en la nueva era de las redes, una de las dificultades principales de los legisladores es el control del movimiento globalizador de la información. Por lo cual, permitir la supresión de la información es un medio de controlar ese movimiento.

La sentencia Google, sentencia del TJUE del 13 de mayo de 2014[63], consagra el derecho al olvido digital o la posibilidad de eliminar los datos de carácter personal en internet cuando se considera que puede perjudicar al ciudadano o desea que sea olvidada al carecer de relevancia actual.

En este caso, se trata de una reclamación efectuada por un ciudadano español que pedía que se eliminasen sus datos que aparecían en un periódico digital y en los buscadores de google afectando a su derecho a la intimidad y su derecho al honor.

---

[61]: Rallo Artemi, *El derecho al olvido en Internet, Google versus España*, Centro de Estudio Políticos y Constitucionales, Madrid, 2014, p. 37

[62]: Ordóñez Solís David, *El derecho al olvido en internet y la sentencia Google Spain*, Revista Aranzadi Unión Europea, pp. 1-1906, 05.2014. La cita transcrita en p. 3.

[63]: STJUE Caso C-131/12 Google Spain, S.L, Google Inc. Vs Agencia Española de protección de datos y Mario Costeja Gonzalez, en http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

Aunque la Agencia Española de Protección de Datos lo desestimó, salvo la indexación de esa noticia por parte de Google, el asunto se remitió a la Audiencia Nacional y esta última a la vista singular del asunto lo elevó al Tribunal Superior de Justicia de la Unión Europea, pronunciando la famosa Sentencia de 13 de mayo de 2014 donde se decidió el derecho del interesado a solicitar la supresión de sus datos en los motores de búsqueda de Google[64].

Así, desde esta sentencia, los usuarios que quieren que un dato personal sea suprimido deben primero solicitar al responsable del tratamiento que analice la información a eliminar y, en el caso de que no se quiera cancelar se podrá acudir ante la propia agencia nacional de protección, la Agencia Española de Protección de Datos aquí en España.

Aunque la sentencia Google glorifica el derecho al olvido, hubo antecedentes jurisprudenciales. El primer intento fue con el Dictamen 1/2008[65] que proclamó la vigencia efectiva del derecho de protección de datos, refiriéndose al derecho a solicitar la supresión de datos de los buscadores de Internet en los siguientes términos[66]:

- Los buscadores deben respetar el derecho a suprimir datos, perfiles personales entre otros
- Los buscadores deben respetar el derecho a suprimir las información incompletas u obsoletas, 'una vez que estos datos no corresponden ya al contenido publicado en Internet por los responsables del tratamiento del sitio o sitios Internet que publican esta información'
- Deber de actualización de las memorias ocultas
- Los editores de webs deben adoptar medidas para informar automáticamente a los buscadores de todas las solicitudes de supresión de datos que reciban

[64]: Puig Carles Ignacio, "Derecho al olvido y el Nuevo Reglamento Europeo", Legalis Consultores, 28.06.2016, en http://www.legalisconsultores.es/2016/06/derecho-al-olvido-y-el-nuevo-reglamento-europeo/

[65]: Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda de 4 de abril de 2008, en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf

[66]: Rallo Artemi, *El derecho al olvido en Internet, Google versus España*, Centro de Estudio Políticos y Constitucionales, Madrid, 2014, p. 175.

Así, podemos decir que el derecho al olvido está relacionado con el deber de actualizar las informaciones. En efecto, el derecho al olvido se manifiesta, entre otros casos, cuando las informaciones son incompletas u obsoletas.

En el caso Times Newspapers vs. UK[67], se proclamó el deber de la prensa de garantizar la exactitud de la información histórica publicada en Internet la cual debe incluir un *"aviso de actualización"*[68].
Así, cuando este deber de actualización no es ejercido por parte de los buscadores y editores, se puede pedir el derecho al olvido por parte de los usuarios.

Podemos concluir que para que el derecho al olvido sea incorporado en un texto europeo con aplicación obligatoria por parte de los Estados Miembros, fue necesario trabajos preliminares.

2. *El objetivo y la reglamentación del derecho al olvido. El resultado a obtener.*

El derecho al olvido está regulado en varios textos legislativos. En España, está regulado en el artículo 18 CE como parte del derecho a la intimidad, pero también al artículo 16 LOPD como 'derecho de rectificación y cancelación'.
En el RGPD, existe una sección que concierne la rectificación y supresión de los datos.

Primero la rectificación se encuentra en el artículo 16. Es una etapa intermedia que permite no llegar hasta la supresión. De hecho, como lo vimos, se puede pedir la supresión de los datos cuando esos son incompletos u obsoletos.

---

[67]: STEDH, Caso Times Newspapers vs. UK de 10 de marzo de 2009
[68]: Rallo Artemi, *El derecho al olvido en Internet, Google versus España,* Centro de Estudio Políticos y Constitucionales, Madrid, 2014, p. 211

Con la rectificación, el operador modifica y completa los datos inexactos[69]. Permite a ambos usuario y operador que las informaciones se queden en la red, pero modificándolas para que sean justas.

Después, llegamos con el articulo 17 al derecho de supresión o derecho al olvido. Vemos la voluntad del legislador de considerar el derecho al olvido como derecho de supresión, en el titulo mismo del artículo: Derecho de supresión («el derecho al olvido»). Sin embargo, el legislador establece límites: no se puede pedir la supresión, en cualquier caso, deben concurrir algunas de las siguientes circunstancias[70]:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo
- el interesado retire el consentimiento en que se basa el tratamiento
- el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento
- los datos personales hayan sido tratados ilícitamente
- los datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento
- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información

Además, el art.17.2 del nuevo Reglamento, establece que "*Cuando haya hecho públicos los datos personales y esté obligado […] a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos*"[71].

[69]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 16
[70]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 17.1
[71]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 17.2

Por tanto, únicamente es de aplicación cuando los datos sean públicos, la tecnología disponible y los costes de aplicación permitan su atención.

Finalmente, se han creado limites a este derecho de olvido. Las solicitudes de supresión no podrán ser aceptadas cuando el tratamiento sea necesario[72]:

- para ejercer el derecho a la libertad de expresión e información
- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la UE o de los Estados miembros que se aplique al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
- por razones de interés público en el ámbito de la salud pública
- con fines de archivo en interés público, investigación científica o histórica o fines estadísticos
- para la formulación, el ejercicio o la defensa de reclamaciones

Por lo cual, vemos que la intimidad recogida al artículo 18 CE se opone a la libertad de expresión recogida al artículo 20 CE. Así, podemos preguntarnos sobre la protección real del derecho al olvido puesto que la libertad de expresión tiene más fuerza que el derecho al olvido.

Finalmente, vemos que los legisladores han querido ir más allá del derecho al olvido porque han también añadido el derecho a la portabilidad de los datos. De hecho, como dije en anterioridad, en los primeros años del desarrollo del derecho al olvido, había una tendencia a confundir olvido y portabilidad de los datos. Aquí, con este nuevo reglamento, vemos una cierta voluntad de aclarar los dos conceptos. En el mismo sentido, se ha introducido un derecho de oposición al artículo 21 del reglamento. Así pues, en este reglamento, se observa la voluntad de los legisladores de introducir y proteger nuevos derechos, aclarando los diferentes conceptos para asegurar una protección real.

[72]: RGPD (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016: Articulo 17.3

No obstante, se puede preguntar sobre la aplicación real y efectiva de este artículo. De hecho, es difícil, por no decir casi imposible, de suprimir una información puesta en la red. Así, se puede preguntar si el dato personal es suprimido o solo escondido para que sea difícil de encontrar. La red funciona un poco como un iceberg: la parte emergida se trata de aquella en la cual se puede encontrar cualquier información con las buenas palabras claves. La parte sumergida es aquella camuflada y desconocida de un gran número de usuarios. Así, ¿los datos son realmente suprimidos o solamente desplazados en esta parte disimulada?

Observamos que los legisladores no son conscientes de esta dificultad de supresión real puesto que hablan solamente de derecho de supresión. Han incorporado esta regla sin estudiar efectivamente si la eliminación era posible o no.

En mi opinión, suprimir datos no es posible. En efecto, la información es demasiado valuosa en el mercado para ser eliminada por parte de los operadores. La incorporación de tal concepto en este texto europeo responde a reivindicaciones ciudadanas y políticas, pero en cualquier caso es una innovación utópica. Los datos serán guardados y escondidos, pero en mi opinión, no serán suprimidos.

B / El establecimiento de una protección especial para los niños

Con el desarrollo de los medios de comunicación y sobre todo del avance del ámbito informático, es crucial establecer textos legislativos que incluyen la protección de los niños. Además de estas herramientas jurídicas, se crean órganos para satisfacer su plena aplicación.

1. La protección de los niños como limite al tratamiento de los datos

Hoy en día, los menores de edad han nacido con un internet muy desarrollado, razón por la cual se les llama 'nativos digitales'[73].

[73]: AEPD, "Internet y menores", en http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2016/internet_y_menores-ides-idphp.php

En efecto, no tuvieron que aprender el uso de la red como nosotros, nuestros padres o abuelos. Nacieron con estos instrumentos, y por eso les es innato el uso de estos dispositivos, se trata de su medio natural.

Sin embargo, aunque los niños sepan utilizar estos medios, antes de una cierta edad, no tienen la madurez necesaria para entender los riesgos y consecuencias que impliquen un uso nefasto y candoroso de la red.

Así, para prevenir tal inseguridad, los legisladores europeos han decidido crear reglas limitativas del tratamiento de los datos cuando estos conciernen menores de edad. Hubo iniciativa parecida, como en la Directiva de servicios de comunicación audiovisual[74]. De hecho, su artículo 12 prevé que *''los Estados miembros adoptarán las medidas adecuadas para velar por que los servicios de comunicación audiovisual a petición ofrecidos por los prestadores del servicio de comunicación bajo su jurisdicción que puedan dañar gravemente el desarrollo físico, mental o moral de los menores se faciliten únicamente de manera que se garantice que, normalmente, los menores no verán ni escucharán dichos servicios de comunicación audiovisual a petición''*[75]. Por lo cual, se ve una voluntad de proteger los niños de ese entorno peligroso.

Mismo contenido está presente al artículo 3 nonies de la Directiva 2007/65/CE del Parlamento Europeo y del Consejo de 11 de diciembre de 2007[76].

---

[74]: Directiva 2010/13/UE del Parlamento y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013&from=ES

[75]: Directiva 2010/13/UE del Parlamento Europeo y del Consejo (Directiva de servicios de comunicación audiovisual): Articulo 12

[76]: Directiva 2007/65/CE del Parlamento Europeo y del Consejo de 11 de diciembre de 2007 por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32007L0065&from=FR

Además, unos años antes de esas dos directivas, tuvimos otra directiva sobre el comercio electrónico y una recomendación sobre la protección de menores y la dignidad humana revisada en 2006 que también tratan de la protección de los menores – art 16 de la directiva[77].

En consecuencia, vemos que el RGPD no es el primer texto que trata proteger a los niños. Sin embargo, se puede creer que esa protección reforzada en el texto estudiado es fruto de presiones de parte de organismos como por ejemplo la UNICEF, organismo de la ONU para la protección de la infancia. De hecho, son organismos que pueden tener una cierta fuerza a la hora de influenciar la redacción de textos legislativos.

Este reglamento, nos expone en sus motivos, las razones de tal legislación sobre los niños. Nos dice que *"los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales"*[78].

Sin embargo, este texto provee una protección individualizada. De hecho, el articulo 8 del reglamento 'Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información', dispone que *"el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó"*[79].

Así, se impone dos límites:

- El tratamiento de los datos de un menor sin el consentimiento de los titulares de la patria potestad es licito cuando el menor tenga como mínimo 16 años.
- Por debajo de esta edad, se necesita el consentimiento del titular de la patria potestad o tutela.

---

[77]: Recommandation sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne, JOUE L 378, p. 72.

[78]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Motivo 38

[79]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 8

Sin embargo, los legisladores han matizado este límite: *"Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años"*[80]. Por lo cual se puede concluir que se necesita siempre el consentimiento de los titulares de la patria potestad hasta que el niño tiene como mínimo 13 años. Los Estados miembros pueden cambiar este mínimo. En España, por ejemplo, la edad mínima no es 16 sino 14 años. Así, cuando el menor tiene 14 años o más, no es necesario el consentimiento de sus padres para que se traten sus datos, de acuerdo con el articulo 13.1 LOPD[81]. Así, en España, los menores entre 14 y 18 años pueden prestar ellos mismos el consentimiento sin necesitar del de sus padres porque se considera que son suficientemente maduros para entender las consecuencias del consentimiento prestado.

No obstante, los legisladores son conscientes de la dificultad de verificar el control hecho por parte de los padres y el consentimiento dado.
Así, han añadido un apartado que deja cierta libertad a los operadores: *"El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible"*[82].
Se habla de 'esfuerzos razonables', por lo cual se deja cierta libertad y margen de maniobra para verificar el consentimiento, no se establece un procedimiento fijo.

Como se deja un margen a los Estados para que fijen el límite mínimo – entre 13 y 16 años – a partir del cual ya no se requiere más el consentimiento de los padres, se ha establecido reglas sobre el consentimiento. En efecto, el articulo 12 nos dice que *"El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información […], así como cualquier comunicación […]*

[80]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 8
[81]: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Articulo 13.1
[82]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 8

relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño"[83].

De hecho, entre 13 y 16 años, no se tiene la misma madurez, por lo cual, un menor que tiene 13 años debe poder entender el cómo se va a tratar sus datos de la misma manera que un menor de 16 años.

Así, vemos que el reglamento se encarga de proteger los niños de este desarrollo digital que puede ser peligroso. Sin embargo, la protección que se hace aquí es mínima. De hecho, podemos dudar de la tutela porque un solo artículo para proteger a la nueva generación que no es siempre consciente de los riesgos de la red puede ser arriesgado.

Además, se ve un desequilibrio en el reglamento, puesto que, en cuento a los niños, los motivos son más desarrollados que los artículos en sí mismo. Por lo cual, el legislador europeo está consciente de que se debe proteger a los niños y desarrolla mucho estos motivos de por qué se debe proteger, pero, a la hora de crear una protección en sí misma, esta es limitada.

También, el hecho de dejar un margen a los operadores a la hora de verificar el consentimiento reduce el ámbito de aplicación del artículo. Además, el hecho que los Estados puedan cambiar la edad mínima a partir de la cual se requiere el consentimiento de los padres – estableciendo un margen de 3 años – debilita la uniformidad del derecho europeo.

Al fin y al cabo, podemos decir que esa protección de los niños establece un límite a los operadores porque restringe el tratamiento de los datos de los niños, pero, no se puede hablar de una defensa tan efectiva que la que concierne el consentimiento, el tema de las transferencias o el olvido, por ejemplo. Tomando el ejemplo español, se puede hablar de una tutela efectiva para los menores de 14 años.

[83]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 12

2. *La creación de instituciones peculiares cuyos órganos vigilan a la buena aplicación del reglamento*

El RGPD, además de haber desarrollado y amplificado las reglas legales referentes a la protección de datos, ha también creado órganos cuyo papel es custodiar la buena aplicación de las reglas generales – consentimiento, tratamiento, transferencias – como de las reglas específicas – derecho al olvido, protección de los niños.

Primero, se ha establecido una norma sobre código de conducta al artículo 40. No se ha creado en sí mismo un código de conducta europeo, paralelo al reglamento, sino que se debe crear en el futuro estos tipos de códigos para *"contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas"*[84].
Estos códigos, redactados y promovidos por los Estados miembros, las autoridades de control, el Comité, la Comisión, las asociaciones y otros organismos tienen como objetivo la ampliación y especificación del reglamento en diferentes sectores[85] como, por ejemplo:

- El tratamiento leal y transparente
- Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
- La recogida de datos personales
- La seudonimización de datos personales
- La información proporcionada al público y a los interesados
- El ejercicio de los derechos de los interesados
- La información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño

[84]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 40.1
[85]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 40.2

En lo que concierne la redacción y 'supervisión del cumplimiento de un código de conducta'[86], no se puede hacer por cualquier organismo. Este debe cumplir con unos requisitos como, por ejemplo *"establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación"*[87] o *"demostrar, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses"*[88].

Finalmente, para que estos textos tengan una cierta fuerza vinculante, se exige que los responsables o encargados del tratamiento adhieren a estos códigos y asumen *"compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados"*[89].

Un sistema parecido está previsto a los artículos 42 y 43 de este nuevo reglamento en lo que concierne la certificación. Tal instrumento permitirá *"en materia de protección de datos y de sellos y marcas de protección de datos, demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"*[90]. De manera similar a los códigos de conductas, los organismos, para crear estos mecanismos de certificación, necesitan acreditar de requisitos y operan solamente en ciertos ámbitos, no son generales.

En paralelo a estos dos mecanismos, existen diferentes órganos con diferentes papeles.

[86, 87, 88]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 41.2
[89]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 40.3
[90]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 42.1

Primero, cada Estado Miembro debe implantar unas autoridades públicas independientes o autoridad de control a fin de *"proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión"*[91]. Esta autoridad debe ser independiente de conformidad con el articulo 52 y su creación debe respetar un procedimiento establecido al artículo 53 (nombramiento, sucesión de autoridades…), y su competencia, funciones y poderes son erigidos a los artículos 55, 56, 57, 58 y 59 del reglamento. Por lo tanto, vemos que esa autoridad de control es muy normalizada en el RGPD.

Después, se regula un Comité Europeo de Protección de Datos, órgano independiente cuyo papel es entre otros[92]:

- asesorar a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento
- llevar un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia
- promover la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control

Además, tiene que redactar un informe anual que debe tener de tema la protección de las personas en lo que concierne el tratamiento de la Unión y en terceros países u organizaciones si es necesario[93].

Como en el caso de la autoridad de control, todo lo que concierne su procedimiento, presidencia, funciones está regulado por el reglamento.

[91]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 51
[92]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 70
[93]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 71

Finalmente, otro órgano que tiene un papel importante, sobre todo en cuento al tratamiento de los datos es el delegado de protección. Esta figura está regulada a los artículos 37 a 39 del reglamento. Tiene un papel más específico que los otros órganos estudiados: asistir al responsable y encargado del tratamiento en lo que concierne este trato de los datos, ofrecer asesoramiento, cooperar con los otros órganos[94]. El reglamento contempla 3 casos en los cuales se debe siempre designar un delegado, pero nos damos cuenta que al final se cubre casi todos los casos[95]:

- el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial
- las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala
- las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales

Por lo cual, el reglamento no solo preceptúa, sino que crea órganos cuya función es vigilar a la buena aplicación del mismo y el respeto de sus normas.

A día de hoy, el reglamento no es plenamente aplicado dado que su entera aplicación está prevista para 2018. Así, nos podemos preguntar si, estos órganos creados por el propio reglamento permitirán en el futuro una aplicación rigorosa del mismo. De hecho, estos órganos son dependientes de los Estados Miembros porque creados por ellos, así, si estos ponen mala voluntad, el papel de los órganos será reducido.

Por lo cual, nos podemos cuestionar sobre otros medios que favorecerían una completa utilización de este nuevo reglamento. Ya está previsto multas administrativas – articulo 84 del reglamento.

---

[94]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 39
[95]: RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016: Articulo 37

De hecho, hoy en día, la política va con la economía y las finanzas. Podemos pensar que, imponiendo multas financieras, se cumplirá el reglamento. Sin embargo, si no se respeta cuyo texto, se deberá encontrar nuevas herramientas más eficaces.

Finalmente, al nivel empresarial, se necesita cambios sobre privacidad para satisfacer con las exigencias legales. De hecho, multas de millones de euros están previstas si no se cumplen las obligaciones reglamentarias. Pero, hay siempre dudas en cuento al cumplimiento de estas normas porque a veces, ciertas empresas prefieren pagar la multa que cambiar sus sistemas internos.

3. El resultado a obtener

El resultado a obtener sería él de un respeto total de estas reglas puesto que los menores son una parte de la población débil, que se debe proteger especialmente.
Hay que verificar que los operadores utilizan todos los medios necesarios para comprobar que en lo que concierne los menores entre 13 y 16 años – según lo establecido por cada legislación nacional – los tutores legales presten su consentimiento, que sean de acuerdo y conscientes acerca del tratamiento de los datos de sus menores.

Este papel de vigilancia lo tiene los órganos presentados al apartado anterior. En lo que les concierne, se debe crear un sistema eficaz para que puedan ejercer sus funciones activamente, proteger efectivamente los ciudadanos europeos y vigilar la buena aplicación del RGPD.

CONCLUSIONES

I. Una protección integral y adaptable a cada nivel

En el Reglamento estudiado, se ve claramente el deseo de los legisladores de adaptar la protección de los ciudadanos a la innovación digital. No se acepta la innovación como excepción a la protección. En efecto, son conscientes del valor pecuniario de los datos, así como de la existencia de un mercado negro poniendo en peligro la seguridad de los usuarios. Por esto, se han creado reglas que siguen siendo generales para abarcar todas las situaciones, pero también unas más específicas para responder a las necesidades del pueblo europeo.

Además, vemos el carácter adaptable de la normativa, en la redacción de los artículos. De hecho, como dije anteriormente, se adapta a las reivindicaciones de los ciudadanos, así como a los conceptos jurídicos en sí. A título ilustrativo, podemos hablar del consentimiento. Tal concepto se ha transformado a fin de arreglarse a la visión actual de la privacidad para poder lograrla. Es una de las nociones en constante cambio, así pues, es imprescindible modificar y acomodar las normas jurídicas para poder lograr una tutela efectiva de los derechos de los ciudadanos.

II. Un Reglamento completo e innovador

Además, se han fortalecido unas bases legales antiguas, pero no siempre respetadas: el consentimiento y las transferencias de datos. Tales nociones son inevitablemente mencionadas y preservadas cuando se trata de la protección de datos. Este reglamento no es una excepción a esa regla; estos conceptos son regulados y fortificados especialmente en el carácter 'claro y efectivo' del consentimiento.
De hecho, con estos nuevos términos, se quiere poner fin al 'reino de las condiciones generales': eran redactadas de tal manera que nadie quería perder tiempo o energía a intentar leerlas.

Con este nuevo reglamento, se trata de aclarar estas condiciones generales, por ejemplo, de modo que cada uno pueda entender en términos claros la futura utilización de sus datos.

También, además de reforzar antiguas normas, este reglamento ha incorporado nuevas, las cuales no han estado reguladas previamente; hablo aquí del derecho al olvido. De hecho, tal derecho se ha desarrollado y normalizado con este reglamento porque ya existía, pero no era incorporado en ningún texto legal europeo. Por lo cual, vemos el deseo de los legisladores de no solamente fortalecer las normas generales, pero también de especificar este reglamento a fin de responder a las exigencias ciudadanas.

Finalmente, se establecen unos límites para asegurar esa protección de datos. Se crean aquí órganos específicos que deben cuidar la ejecución del reglamento, pero también normas protectoras de los usuarios más débiles, como los menores. Eso se revela esencial a la elaboración de un texto positivo y seguro.

III. Una aplicación total dudosa

La redacción de tal normativa era fundamental puesto que el último texto sobre el asunto remonta al año 1995. Sin embargo, podemos dudar de su aplicación en la práctica. De hecho, puesto que es un reglamento, no se necesita transposición en los ordenamientos jurídicos internos. El hecho de haber preferido un reglamento a una directiva nos muestra que los legisladores europeos quieren una aplicación fija y estricta de esas normas. No obstante, dado que establece nuevas reglas, se ha decidido poner un plazo para que los Estados miembros puedan adaptar su legislación interna a la entrada en vigor de este reglamento. Sin embargo, aunque su plena aplicación esta prevista dentro de un poco más de un año (25 de mayo de 2018) los Estados miembros tardan en modificar sus legislaciones internas.
A título de ejemplo, Francia o España no han empezado este trabajo. Uno de los Estados quien realmente ha empezado es Alemania.

Finalmente, se prevé sanciones económicas si no se respeta las nuevas normas. Pero, no podemos asegurar que las empresas prefieran cambiar sus políticas y funcionamiento interno antes que pagar. De una manera sintética, podemos decir que este texto es muy completo y protector, pero hay que esperar unos años para comprobar su verdadera eficacia y respeto.

BIBLIOGRAFIA [bibliografía consultada el 11.05.2017]

Libros y material digital

-ANGEL MENDOZA Miguel, "¿Cuánto por esa cuenta? El valor de la información en el mercado negro", WeLiveSecurity, 25.11.2016, en http://www.welivesecurity.com/la-es/2016/11/25/informacion-mercado-negro/

-BROCCA Marina, "El nuevo reglamento de protección de datos", Protección de datos, 20.10.2016, en https://marinabrocca.com/proteccion-de-datos/nuevo-reglamento-proteccion-datos/

-CAZURRO BARAHONA Víctor, *Transferencias internacionales de datos*, en http://www.aranzadi.es/sites/aranzadi.es/files/creatividad/Publicaciones/email_practicucm_proteccion_datos_2016/images/CapituloPracticumPDatos2015.pdf

-DE LA HIGUERA Ana, "El mercado negro de la información y el nuevo Reglamento de Protección de Datos", KPMG Blogs, 22. 11. 2016, en http://www.kpmgblogs.es/el-mercado-negro-de-la-informacion-y-el-nuevo-reglamento-de-proteccion-de-datos/

-FRAGUAS MADURGA Lourdes, *El concepto de derechos fundamentales y las generaciones de derechos*, *Anuario del Centro de la Universidad Nacional de Educación a Distancia en Calatayud. N.o 21*, pp. 117-136, 2015, en http://www.calatayud.uned.es/web/actividades/revista-anales/21/03-05-LourdesFraguasMadurga.pdf

-Gobierno de España, Ministerio de Industria, Turismo y Comercio, "Normativa sobre protección de datos personas: catálogos y requisitos agrupados por materias", ISMS Fórum Spain, en http://www.protegetuinformacion.com/docs/13/lopd_PDF_tema1_proteccion_datos_personales.pdf

-LASSERRE Bruno, *Le point de vue de l'autorité française de la concurrence*, en ALMUNIA, Joaquim ("et al "), New Frontiers of antitrust 2013, Competition Law in times of Economic, Bruylant, 2013

-LÓPEZ CARBALLO Daniel, "Responsabilidades derivadas del tratamiento y explotación de los datos personales", 27.01.2017, en http://dlcarballo.com/2017/01/27/responsabilidades-derivadas-del-tratamiento-y-explotacion-de-los-datos-personales/

-ORDÓÑEZ SOLÍS David, *El derecho al olvido en internet y la sentencia Google Spain*, Revista Aranzadi Unión Europea 6, Junio 2014

-POZZI Sandro, "Yahoo anuncia el robo de datos de mil millones de cuentas", El Pais, 15.12.2016, en

http://tecnologia.elpais.com/tecnologia/2016/12/14/actualidad/1481753868_540005.html

-PUIG CARLES Ignacio, "Derecho al olvido y el Nuevo Reglamento Europeo", Legalis Consultores, 28.06.2016, en http://www.legalisconsultores.es/2016/06/derecho-al-olvido-y-el-nuevo-reglamento-europeo/

-QUINCOCES RIESCO Amaya, "¿Cuánto valen los datos personales en el mercado del ciberdelito?", Mercado Ciberdelito, EfeFuturo, 28.09.2015, en http://www.efefuturo.com/noticia/cuanto-valen-los-datos-personales-en-el-mercado-del-ciberdelito/

-RALLO Artemi, *El derecho al olvido en Internet, Google versus España*, Centro de Estudio Políticos y Constitucionales, Madrid, 2014

-RECIO GAYO Miguel, *Protección de datos personales e innovación: ¿(in)compatibles?*, en Reus Editorial, Derecho de las nuevas tecnologías, 2016, p. 5

-RISON Alice, "Microsoft Cloud is first CSP behind the Privacy Shield", Microsoft Azure, 26.09.2016, en https://azure.microsoft.com/en-us/blog/microsoft-cloud-is-first-csp-behind-the-privacy-shield/

-SANCHO VILLA Diana, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003,

-VELASCO Oscar, "El costo de la información en el mercado negro", E.Security, 15.01.2015, en http://revistaesecurity.com/el-co/

-ZABALLOS PULIDO Emilia, tesis doctoral en http://eprints.ucm.es/22849/1/T34733.pdf

Legislación

-Directiva 95/46/CE, "Protección de los datos personales", en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al14012

-Directiva 2007/65/CE del Parlamento Europeo y del Consejo de 11 de diciembre de 2007 por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32007L0065&from=FR

-Directiva 2010/13/UE del Parlamento y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de

comunicación audiovisual (Directiva de servicios de comunicación audiovisual), en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013&from=ES

-Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

-Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666

-Reglamento (UE) 2016/679 del Parlamento 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)

Jurisprudencia

-STJUE Caso C-101/01, Bodil LindqvistL, de 6 de noviembre de 2003, en : http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d6b3e72d7f664a440d9956b8b3324e9058.e34KaxiLc3eQc40LaxqMbN4Pax0Ke0?text=&docid=48382&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=30433

-STEDH, Caso Times Newspapers vs. UK de 10 de marzo de 2009

-STJUE, Caso C-521/11, Amazon, de 11 de julio de 2013, en http://curia.europa.eu/juris/document/document.jsf?text=&docid=139407&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=109092

-STJUE Caso C-131/12 Google Spain, S.L, Google Inc. Vs Agencia Española de protección de datos y Mario Costeja Gonzalez, de 13 de mayo 2014, en http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

-Sentencia de la TEDH Caso no 61838/10, Vukota-Bojić v. Switzerland, de 18 de octubre de 2016, en http://hudoc.echr.coe.int/fre#{"itemid":["001-167490"]}

-STJUE Asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department, de 21 de diciembre de 2016, en, http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=ES

Otra documentación

-Agencia Española de Protección de Datos, Calidad de datos, “Principios relativos a la calidad de los datos”, en https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/calidad_de_datos/index-ides-idphp.php

-Agencia Española de Protección de Datos, “Cuestiones sobre cumplimiento del apartado de transferencias internacionales”, en

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_cumplimiento/index-ides-idphp.php

-Agencia Española de Protección de Datos, "Transferencias internacionales de datos", en https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

-Agencia Española de Protección de Datos, "Principales derechos", en http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php

-Agencia Española de Protección de Datos, "Derecho al olvido", en http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

-Comunicación de la Comisión Europea de 4 de noviembre de 2010 sobre "un enfoque global de la protección de datos personales en la Unión Europea: el olvido como 'cancelación' de datos personales, en http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009

-ConfiLegal, "Las nuevas normas de protección de datos aprobadas por el Parlamento Europeo devuelven su control a los ciudadanos", 14.04.2016, en https://confilegal.com/20160414-las-nuevas-normas-proteccion-datos-devuelven-control-los-ciudadanos/
-Definición de la intimidad, 2014, en http://definicion.de/intimidad/

-"Dans un arrêt, la CJUE estime que les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications électroniques", Droits fondamentaux, lutte contre la discrimination - Justice, liberté, sécurité et immigration, EuropaForum, 21.12.2016, en http://www.europaforum.public.lu/fr/actualites/2016/12/cjue-donnees/index.html

-Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda de 4 de abril de 2008, en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf

-Les usages variés du Net, IAB France, en http://www.iabfrance.com/contenu/dossiers/fiches/les-usages-varies-du-net

-Los peligros del modelo cloud computing, CSO Digital, ComputerWorld, 22.09.2008, en http://cso.computerworld.es/cloud/los-peligros-del-modelo-cloud-computing

-Recommandation sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité del 'industrie européenne des services audiovisuels et d'information en ligne, JOUE L 378, p. 72.