Implicaciones geográficas del nuevo Reglamento General de Protección de Datos

Aplicación a la geoinformación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas sobre tratamiento de datos personales.

DÍAZ DÍAZ, Efrén

La Directiva europea de Protección de Datos de 1995, tras veinte años de vigencia, ha sido derogada por la aprobación de un nuevo y relevante Reglamento General de Protección de Datos (RGPD). Su ámbito de aplicación es europeo y tiene efecto directo en cada Estado miembro. Su objetivo es superar la fragmentación normativa existente y modernizar los principios de privacidad en la Unión Europea.

El texto definitivo, confirmado por el Comité de Representantes Permanentes (Coreper), ha quedado publicado el 25 de mayo de 2016 para entrar en vigor dos años más tarde, el 25 de mayo de 2018.

El RGPD constituye un conjunto unitario y actualizado de reglas aplicables en todo el territorio de la Unión Europea y para todo el procesamiento de datos de ciudadanos europeos. Evitará así la fragmentación del mercado dentro de la Unión, derivada de la transposición a las legislaciones nacionales de la Directiva sobre protección de datos de 1995, y facilitará la actividad empresarial y corporativa transfronteriza, la libre circulación de datos personales y la mayor garantía de los derechos y libertades fundamentales de los ciudadanos europeos. En interés de los ciudadanos europeos, regula particularmente los derechos de acceso, rectificación, cancelación y oposición, junto al reconocimiento de dos nuevos derechos: el derecho al olvido digital y la portabilidad de datos.

En el ámbito particular de la geoinformación, el RGPD incluye relevantes novedades, y significativamente define entre los «datos personales» toda información sobre una persona física identificada o identificable, incluido no sólo cualquier identificador como, por ejemplo, un número de identificación, sino también los datos de localización. Asimismo, la nueva norma presta particular atención a la «elaboración de perfiles», donde incorpora toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física y, en el ámbito geoespacial, alude expresamente a la ubicación o movimientos de dicha persona física.

PALABRAS CLAVE

Geoinformación, Protección de Datos, Ubicación, Localización, Datos Espaciales, Interoperabilidad jurídica.

AUTOR

Efrén DÍAZ DÍAZ
efrendiaz@mascalvet.com
Bufete Mas y Calvet
Departamento de Derecho Administrativo, Tecnológico y Geoespacial

1. Antecedentes.

1.1. Directiva sobre protección de datos de 1995.

La Directiva 95/46/CE (*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.*, 1995)[1], tras veinte años de vigencia, precisa de un marco jurídico nuevo, coherente y homogéneo, para garantizar el derecho fundamental a la protección de datos en la Unión Europea[2].

Las incongruencias en la protección de los datos personales en los distintos Estados de la Unión han puesto de relieve, también para la Comisión Europea, la necesidad de disponer de una regulación unitaria y armonizada de protección de datos en todo el territorio de la Unión, en particular para suprimir o reducir el margen de elección de los legisladores nacionales y de las autoridades de control y los Tribunales.

Conscientes del problema que supone la fragmentación de la normativa de protección de datos en Europa, por las diferencias legislativas y de aplicación de la regulación entre los Estados miembros, el Tribunal de Justicia ha reiterado la importancia del objetivo perseguido por la Directiva 95/46/CE, centrado en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad[3].

Sin embargo, la Directiva 95/46/CE no ha garantizado plenamente ninguno de sus dos objetivos principales.

En primer término, el derecho a la protección de datos de carácter personal, consagrado en el art. 8 de la Carta Europea de Derechos Fundamentales[4], no ha visto garantizado el mismo nivel de protección en todos los Estados miembros ni en las distintas entidades y corporaciones. A ello ha contribuido incisivamente el hecho de que las tecnologías de la información y las comunicaciones, cada vez más instantáneas, han facilitado la comunicación de datos personales de modo prácticamente inmediato más allá de las fronteras nacionales y de la Unión Europea.

La aplicación efectiva de las normas protectoras de la privacidad, concretada en el derecho del ciudadano al control de su información personal, ha venido a exigir un mayor nivel de cooperación entre las autoridades de protección de datos de los diferentes Estados miembros. Asimismo, la Unión Europea actualmente se encuentra en mejores condiciones para garantizar la tutela efectiva de los derechos de los ciudadanos europeos, también frente a tratamientos de sus datos que se realizan fuera de las fronteras del Espacio Económico Europeo (EEE)[5], que las iniciativas adoptadas individualmente por cada uno de los Estados.

---

[1] 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. (1995). Directiva 95/46/CE. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995L0046. DOUE n° L 281 de 23/11/1995 p. 0031 - 0050.

[2] El concepto actual de privacidad hunde su raíz en los Estados Unidos de América, donde el juez americano Thomas Cooley asentó en 1888 la definición de privacidad como «*the right to be let alone*» (Cooley & Lewis, 1907 Cooley, T. M., & Lewis, J. (1907). *A treatise on the law of torts or the wrongs which arise independently of contract*. Chicago: Callaghan & Co. Retrieved from http://books.google.com/books?id=ZmQ9AAAAIAAJ), el derecho a ser dejado solo, a ser dejado en paz. Por ello, el estudio de la regulación europea precisa conocer el origen de este importante derecho, hoy ya reconocido y consagrado como derecho fundamental y autónomo en la Carta de los Derechos Fundamentales de la Unión Europea (*Carta de los Derechos Fundamentales de la Unión Europea* (2010). CDFUE. Recuperado a partir de http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003).

[3] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de noviembre de 2003 (C-101/01 - Bodil Lindqvist) (2003). http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1129584.

[4] Carta de los Derechos Fundamentales de la Unión Europea (2010). CDFUE. Recuperado a partir de http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003.

[5] El Espacio Económico Europeo (EEE) incluye los Estados de la Unión Europea, Islandia, Liechtenstein y Noruega. Cfr. http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_6.5.3.html

En segundo término, la diversidad de enfoques nacionales sobre la efectividad de la protección de datos personales ha constituido un obstáculo para el desarrollo y expansión del mercado interior. Como ha destacado el Tribunal de Justicia en la Sentencia *Lindqvist*, las diferencias entre los regímenes nacionales aplicables al tratamiento de datos personales pueden afectar seriamente al establecimiento y al funcionamiento del mercado interior.

Ante esta situación, en la Unión Europea se ha hecho necesario establecer una regulación más transparente y una unidad de aplicación del Derecho europeo que imponga a los responsables y encargados de tratamiento el mismo nivel de obligaciones, una supervisión coherente y unas sanciones equivalentes en todo el territorio de la Unión. Junto a las disparidades actuales que impiden a las organizaciones multinacionales desarrollar políticas paneuropeas sobre protección de datos, los diversos operadores y, en particular, los sociales y económicos, han requerido una mayor seguridad jurídica que permita efectuar las transferencias de datos personales a través de las fronteras interiores de la UE, algo incompatible con la actual fragmentación de las legislaciones nacionales.

El desarrollo de la economía digital en la Unión Europea precisa actualmente un marco coherente y jurídicamente armonizado para la protección de datos personales en todos los Estados miembros. Además, la integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de flujos transfronterizos y del consiguiente intercambio de datos entre operadores económicos y sociales, públicos y privados.

La necesidad de garantizar el derecho fundamental a la protección de datos de carácter personal y su aplicación homogénea en el contexto de todas las políticas de la UE han conducido a la Comisión a proponer *«una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal»*[6].

En este sentido, si bien el marco jurídico actual sigue siendo adecuado en sus objetivos y principios, no ha logrado evitar la fragmentación en la aplicación en la Unión del derecho fundamental a la protección de datos de carácter personal, ni tampoco la inseguridad jurídica ni la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea[7].

Como ha destacado la Propuesta de Reglamento General de protección de datos (2012)[8], *«ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas»*.

1.2. Propuesta de Reglamento General de Protección de Datos (2012).

La reforma europea de la protección de datos es un conjunto legislativo que la Comisión Europea propuso en 2012 para actualizar y modernizar la normativa sobre protección de datos. Afecta a dos instrumentos legislativos: el Reglamento General de protección de datos, destinado a sustituir la Directiva 95/46/CE, y la Directiva sobre protección

[6] Cfr. la Comunicación de la Comisión titulada «*Un enfoque global de la protección de los datos personales en la Unión Europea*» -COM (2010) 609 final- y el Plan de acción de la Comisión por el que se aplica el Programa de Estocolmo -COM (2010) 171 final-.

[7] *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*. (2010). Recuperado a partir de http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm.

[8] Propuesta de Reglamento General de protección de datos (2012). Disponible en: http://eur-lex.europa.eu/procedure/ES/2012_11?rid=1&qid=1443173807357

de datos en el ámbito judicial y policial, destinada a sustituir la Decisión marco sobre protección de datos de 2008, objeto del «Tercer Pilar»[9].

En este estudio nos centraremos en el Reglamento General por su mayor incidencia en la protección de la privacidad de las personas físicas y su repercusión jurídica práctica para ciudadanos y entidades.

No obstante, previamente conviene aclarar que la Directiva sobre protección de datos en el ámbito policial tendrá por objeto proteger los datos personales tratados con fines no sólo de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, sino también con fines de protección y prevención frente a amenazas contra la seguridad pública. La garantía de un nivel uniforme y elevado de protección de los datos personales de las personas físicas es fundamental, al tiempo que se facilita el intercambio de datos personales entre las autoridades policiales de los distintos Estados miembros. La nueva Directiva se aplicará tanto al tratamiento transfronterizo de datos personales como al procesamiento de datos personales por las autoridades policiales y judiciales en el ámbito meramente nacional. La Decisión marco actual, que quedará sustituida por la nueva Directiva, cubría únicamente el intercambio transfronterizo de datos.

Tras años de trabajo legislativo, el Parlamento Europeo ha aprobado en abril de 2016 el citado *Reglamento del Parlamento Europeo 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* (RGPD en adelante), que entrará en vigor 20 días después de su publicación en el Diario oficial de la UE (European Commission, 2016)[10]. Sus disposiciones serán de aplicación directa en todos los Estados miembros dos años después. Los países tendrán un plazo de dos años para trasladar los cambios normativos a la legislación nacional.

El *Reglamento General* pretende establecer una regulación armonizada en todos los Estados de la Unión Europea, con la consiguiente derogación de las normas nacionales específicas[11]. Se fundamenta en la aplicación del principio de subsidiariedad normativa de los Estados miembros, con el objetivo de superar la aproximación fragmentaria de la Directiva 95/46/CE.

El RGPD incorpora un conjunto unitario de reglas aplicables en toda la UE y tiene como objetivo actualizar el marco regulatorio, dados los profundos cambios que han tenido lugar en cuanto a la forma en que se recopilan, almacenan y procesan los datos personales.

En este sentido, el Reglamento mantiene los derechos de acceso, rectificación, cancelación y oposición y, como novedad, incorporará dos derechos de nueva creación, el «derecho al olvido» (o supresión) y el «derecho a la portabilidad de datos». Asimismo, aborda nuevas cuestiones como la creación de perfiles o la seudonimización, e incorporará los principios del análisis de riesgos y la «privacidad por defecto y por diseño». Además, el ámbito de aplicación del RGPD se extenderá más allá de las fronteras de la UE y afectará a organizaciones, entidades y empresas que, aunque no estén establecidas en territorio europeo, ofrezcan bienes y servicios a residentes de la UE o monitoricen sus conductas de comportamiento[12].

---

[9] El Tercer Pilar comprende la cooperación policial y judicial en materia penal, regulada por el Título VI del TUE («DOUE» núm. 83, de 30 de marzo de 2010, páginas 47 a 199 (153 págs.), Unión Europea, Referencia: DOUE-Z-2010-70006).

[10] European Commission. (2016). *Reforma de la protección de datos – Nuevas reglas adaptadas a la era digital*. Accesible en http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/Reforma-de-la-protecci%C3%B3n-de-datos-%E2%80%93-Nuevas-reglas-adaptadas-a-la-era-digital.

[11] El desarrollo del procedimiento legislativo y su evolución normativa puede seguirse a través del Parlamento Europeo. Disponible en: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en y en http://eur-lex.europa.eu/procedure/ES/2012_11?rid=1&qid=1443173807357.

[12] El Special Eurobarometer 359 publicado en junio de 2011 ((*Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*, 2010), reveló información significativa sobre el escenario europeo actual, pues sólo el 26% de los usuarios de redes sociales controlan sus datos, el 74% de los

En este ámbito, *«la Comisión Europea ha decidido proponer un marco legislativo sólido y coherente que cubre todas las políticas de la Unión, refuerza los derechos individuales, potencia la dimensión de mercado único de la protección de datos y reduce los trámites burocráticos engorrosos para las empresas»* (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *La protección de la privacidad en un mundo interconectado, Un marco europeo de protección de datos para el siglo XXI*, 2012)[13].

La citada Comunicación aboga también por la protección de los derechos en un contexto de globalización, y sostiene que *«La protección de los derechos de los ciudadanos debe extenderse a la transferencia de datos personales de la UE a terceros países y a toda actividad que se dirija a los ciudadanos de los Estados miembros y en el marco de la cual sus datos sean utilizados o analizados por proveedores de servicios de terceros países. Esto significa que las normas de protección de datos de la UE deben aplicarse con independencia de la ubicación geográfica de una empresa o de su centro de tratamiento de datos»*[14].

La Comisión Europea además es plenamente consciente de que en el contexto de globalización actual los datos personales se transfieren a través de un creciente número de fronteras virtuales y geográficas y se conservan en servidores ubicados en numerosos países. En consecuencia, es necesario actualizar el alcance y el ámbito de aplicación objetivo de las normas europeas en esta materia.

En definitiva, como afirma una de las primeras conclusiones de la Comisión Europea, *«La reforma de la protección de datos de la UE pretende configurar un marco moderno, sólido, coherente y global de protección de datos para la Unión Europea que reforzará el derecho fundamental de los ciudadanos a la protección de sus datos. Se respetarán otros derechos como la libertad de expresión e información, los derechos del niño, el derecho a la actividad empresarial, el derecho a un juicio justo y el secreto profesional (por ejemplo, para la abogacía), así como el estatuto jurídico de las iglesias conforme a la legislación de los Estados miembros»*[15].

El reto tecnológico y jurídico que representa actualmente el desarrollo, expansión y popularización de la Red de redes y de sus numerosas aplicaciones tecnológicas precisa necesariamente una aproximación global por su naturaleza transversal o multipropósito y su alcance internacional. No hay duda de que asistimos a la regulación en privacidad de mayor calado para los años venideros, con nuevas reglas legales, el reconocimiento de derechos fundamentales y de principios de calidad de los datos y habilitación legítima para el tratamiento, motivada por la urgencia de una regulación estable que conforme las sociedades futuras en entornos digitalizados y de procesamiento masivo y transfronterizo de información personal.

La actual revisión de instrumentos internacionales en privacidad alcanza a todos los niveles de gobierno y organización, no sólo en Europa, sino también en entornos internacionales y sectoriales, además de corporativos.

---

europeos considera la divulgación de información personal parte creciente de la vida moderna, el 43% de los usuarios de Internet ha pedido más información personal de la necesaria, sólo el 33% de los europeos conoce la existencia de las autoridades nacionales de protección de datos y, de forma muy llamativa, el 90% de los europeos quieren los mismos derechos de protección de datos en toda la UE.

[13] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, La protección de la privacidad en un mundo interconectado, Un marco europeo de protección de datos para el siglo XXI. (2012). (COM 2012) 9 final, 25 de enero de 2012. Accesible en: http://register.consilium.europa.eu/doc/srv?l=ES&f=ST%205852%202012%20INIT

[14] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *La protección de la privacidad en un mundo interconectado, Un marco europeo de protección de datos para el siglo XXI*, (COM 2012) 9 final, 25 de enero de 2012, pg. 11.

[15] Cfr. Conclusiones de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (COM 2012) 9 final, 25 de enero de 2012.

En este sentido, el marco global de la privacidad también queda delimitado por los principios de toda sociedad democrática y respetuosa con los derechos fundamentales, pues sin la privacidad, como afirma Piñar Mañas, *«no puede hablarse ni de respeto a la dignidad ni de libertad»* (Piñar Mañas, 2008)[16]. Además, hoy en día la privacidad se encuentra sujeta a diversas tensiones, incluso retos, en relación con la libertad de expresión, con la transparencia y acceso a la información, con los intereses y evolución del mercado y con la lucha por la seguridad ciudadana (Piñar Mañas & Canales Gil, 2008)[17].

2. Regulación de la privacidad en Estados Unidos de América.

El concepto originario de «privacy» fue desarrollado por los jueces Warren & Brandeis en su conocido artículo *«The Right to Privacy»* (Warren & Brandeis, 1890)[18], pues afirmaron que *«In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent»*.

Después de explicar cómo el ejercicio del derecho ha de ser atemperado con la debida ponderación de otros derechos concurrentes, ambos Magistrados concluyeron que *«The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise»*.

Este concepto, todavía digno de ser tenido en cuenta, ha sido desarrollado en la actualidad tras las modernas regulaciones sobre privacidad y protección de datos personales. Sin embargo, en su momento, Warren & Brandeis se vieron compelidos a poner coto a una situación personal en que se había encontrado la esposa de uno de ellos, quien sufrió la invasión de su vida privada por diversos periodistas, y formularon un nuevo derecho de gran interés y con elocuencia:

> *«This development of the law was inevitable. The intense intelectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature»*.

En un primer momento el derecho a la privacidad actuaba sólo frente a las interferencias físicas de la vida y la propiedad. Gradualmente, y desde mediados del siglo XX, el objeto de los derechos se fue ampliando y, en la actualidad, el derecho a la vida ha pasado a significar *derecho a disfrutar de la vida*, que incluye el citado *derecho a estar solo*.

Como sostiene Piñar Mañas, *«el derecho debe preservarnos frente a las invasiones de los «sagrados límites de nuestra vida privada y doméstica». El derecho a la privacidad supone, pues, el derecho a poder estar solo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir injerencias no deseadas y sin interferir en el derecho de los demás»* (Piñar Mañas, 2008)[19].

Por ello conviene tener en cuenta estos antecedentes específicos que contextualizan la actual regulación norteamericana en materia de privacidad en general y de protección de datos personales, en particular, por la influencia que también ejercen fuera de los Estados Unidos.

---

[16] Piñar Mañas, J. L. (2008). *¿Existe la privacidad?* Madrid: Universidad CEU San Pablo, Lección magistral impartida en la Apertura Solemne del Curso Académico, p. 19.
[17] Piñar Mañas, J. L., & Canales Gil, A. (2008). Legislación de protección de datos. Madrid: Iustel., págs. 91 y ss.
[18] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890) (pp. 193-220), p. 195. Accesible en: http://www.jstor.org/stable/1321160
[19] Cfr. Piñar Mañas, J. L. (2008). *¿Existe la privacidad?* Madrid: Universidad CEU San Pablo. Lección magistral impartida en la Apertura Solemne del Curso Académico, p. 26 y 27.

2.1. «Consumer Privacy Bill of Rights».

2.1.1. Proyecto integral para la privacidad de los consumidores.

El Gobierno de los Estados Unidos de América aprobó el 23 de febrero de 2012 la *Consumer Privacy Bill of Rights* (States. & Office., 2012)[20], fruto de una reacción legislativa directa, en menos de un mes, tras la aprobación el 25 de enero de 2012 de la propuesta europea de *Reglamento General de Protección de Datos*.

Mientras que la *Consumer Privacy Bill of Rights* (23/02/2012) establece reglas claras para los consumidores en la Economía Digital y se inspira en los principios de seguridad, confianza e innovación, el *Reglamento General de Protección de Datos* (25/01/2012) reafirma la garantía de un nivel adecuado de protección de la privacidad del ciudadano en toda la Unión Europea[21], junto al reconocimiento de derechos de acceso, rectificación, cancelación y oposición, y la regulación de nuevos derechos como el derecho al olvido digital (art. 17 RGPD) y la portabilidad de datos (art. 18 RGPD).

No obstante, las relaciones en materia de privacidad entre la Unión Europea y Estados Unidos atraviesan un momento delicado, aunque la Comisión de la UE y los Estados Unidos han acordado un nuevo marco para los flujos transatlánticos de datos, denominado el *«Escudo de la privacidad UE - EE.UU»*[22].

La *Consumer Privacy Bill of Rights* forma parte de un proyecto norteamericano integral para mejorar la protección de la privacidad de los consumidores y garantizar que Internet siga siendo un motor para la innovación y el crecimiento económico.

---

[20] Cfr. States., U., & Office., W. H. (2012). Consumer data privacy in a networked world a framework for protecting privacy and promoting innovation in the global digital economy. Washington [D.C.]: The White House. Retrieved from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[21] Cfr. *Advocate General Considers EU-U.S. Safe Harbor to be Invalid*. (2015). Retrieved September 25, 2015, from http://www.natlawreview.com/article/advocate-general-considers-eu-us-safe-harbor-to-be-invalid and http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=401385. Cfr. Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 (C-362/14 - Schrems) (2015). Accesible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=523715.

Esta importante sentencia declara que *«El artículo 25, apartado 6, de la de la 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 su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado».*

En definitiva, el TJUE en su Sentencia de 6 de octubre de 2015 ha declarado que *«La Decisión 2000/520 es inválida»*.

[22] Cfr. European Commission. (2016). *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (IP/16/216)*. Recuperado a partir de http://europa.eu/rapid/press-release_IP-16-216_en.htm. También European Commission. (2016). *Recuperar la confianza en los flujos de datos transatlánticos gracias a salvaguardias estrictas: la Comisión Europea presenta el Escudo de la privacidad UE-EE UU (IP/16/433)*. Recuperado a partir de http://europa.eu/rapid/press-release_IP-16-433_es.htm. Díaz Díaz, E. y V. (2016). *Max Schrems: «El escudo de privacidad UE-EEUU volverá directamente a la corte de Luxemburgo»*. Recuperado 4 de marzo de 2016, a partir de http://www.lawyerpress.com/news/2016_03/0103_16_001.html.

El proyecto legislativo guiará los esfuerzos para dar a los usuarios norteamericanos más control sobre cómo se utiliza su información personal en Internet y ayudar a las empresas a mantener la confianza de los consumidores y crecer en un entorno digital en rápida evolución.

Además, las principales compañías de Internet y las redes de publicidad en línea se comprometen a aplicar la tecnología del *«Do Not Track»* en la mayoría de los principales navegadores de Internet para facilitar a los usuarios el control del seguimiento en línea. Las compañías que representan la difusión de casi el 90 por ciento de los anuncios según el comportamiento de los usuarios en línea, como Google, Yahoo!, Microsoft y AOL, han acordado cumplirlo cuando los consumidores eligen controlar el seguimiento en línea[23].

Las compañías que suscriben este compromiso estarán sujetas a la supervisión de la Federal Trade Commission («FTC», 2015)[24].

> *«American consumers can't wait any longer for clear rules of the road that ensure their personal information is safe online»*, afirmó el Presidente Obama[25]. *«As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint, companies, consumer advocates and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth»*.

En este marco, la industria norteamericana de la publicidad también se comprometió a no publicar los datos de navegación de los consumidores que las empresas puedan utilizar para finalidades distintas de la publicidad, al igual que los empresarios que toman decisiones de contratación o aseguradores que determinan la cobertura.

Como sostuvo el presidente de la FTC, Jon Leibowitz, *«It's great to see that companies are stepping up to our challenge to protect privacy so consumers have greater choice and control over how they are tracked online. More needs to be done, but the work they have done so far is very encouraging»*.

2.1.2. Un proyecto de ley de privacidad del consumidor.

La *Consumer Privacy Bill of Rights* busca establecer un marco para la protección de la privacidad y la promoción de la innovación en la economía digital mundial, consciente de que representa un papel fundamental en el crecimiento económico sostenible y en el desarrollo de la propia sociedad del conocimiento.

El punto de partida de esta norma estadounidense se encuentra en que todos los días, millones de ciudadanos van a la tienda, al taller, al banco, aprenden, hablan y trabajan en línea. Según datos publicados por la FTC, a la vuelta del siglo XX, las ventas minoristas en línea representaban alrededor de 20 mil millones de dólares en los Estados Unidos, ahora están llegando a 200 mil millones de dólares.

[23] El "Do Not Track" es una propuesta de la tecnología y la política que permite a los usuarios optar por el no seguimiento de los sitios web que se visitan, incluyendo los servicios de análisis, redes de publicidad y las plataformas sociales. En la actualidad algunos de los sitios web ofrecen un seguimiento fiable y permiten activar el "no seguimiento" mediante herramientas para bloquear, pero no siempre son fáciles de usar ni integrales. Al igual que el popular "Do Not Call registry", el servicio "Do Not Track" impide seguir la pista a los cibernautas y proporciona a los usuarios una opción simple y persistente de optar por el no seguimiento en las web de terceros.
[24] Federal Trade Commission, disponible en: http://www.ftc.gov/.
[25] The White House. (2012). We Can't Wait: Obama Administration Unveils Blueprint for a «Privacy Bill of Rights» to Protect Consumers Online. Office of the Press Secretary. Washington [D.C.]. Recuperado a partir de https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

Internet se ha convertido en un motor de la innovación, de crecimiento empresarial y de creación de empleo, por lo que esta norma pretende establecer una base sólida de protecciones claras para los consumidores y un conjunto de principios básicos y de políticas de privacidad para ayudar a las empresas a orientar sus decisiones en esta materia cada vez más estratégica. En otras palabras, el proyecto de ley americana fija una línea de base de indispensables protecciones para los consumidores y una mayor seguridad para las empresas.

2.2. Reconocimiento de derechos.

La nueva norma americana se aplicará a los datos personales, entendidos como cualquier dato, incluida la agregación de datos, vinculado a una persona física individual. Dato personal puede comprender datos de ordenadores o de cualesquiera dispositivos específicos.

La Administración norteamericana adopta la legislación federal que asume y aplica los principios de la *Consumer Privacy Bill of Rights*. Incluso sin legislación, la Administración establecerá un proceso para que múltiples partes interesadas puedan utilizar los derechos que la nueva norma define como un modelo para códigos de conducta que son exigibles por la Comisión Federal de Comercio (FTC).

Estos elementos, desde la nueva Ley y los códigos de conducta, hasta mecanismos vinculantes, incrementarán la interoperabilidad en el marco de la privacidad de los datos de los consumidores americanos y los de sus socios internacionales. En particular, la *Consumer Privacy Bill of Rights* reconoce derechos a los consumidores.

Entre otros, los siguientes: 1) *control del individuo*, pues los consumidores tienen derecho a ejercer el control sobre los datos personales que las organizaciones recogen de ellos y a conocer cómo los utilizan; 2) *transparencia*, ya que los consumidores tienen derecho a una información fácilmente comprensible sobre las prácticas de privacidad y seguridad; 3) *respeto del contexto*: los consumidores tienen derecho a que las organizaciones procedan a recopilar, utilizar y revelar datos personales de manera coherente con el contexto en el que los consumidores suministran los datos, sin destinarlos a finalidades distintas ni incompatibles; 4) *seguridad*: los consumidores tienen derecho a asegurar y manejar de forma responsable los datos personales en las plataformas tecnológicas puestas a disposición por las empresas (que deben evaluar los riesgos para la privacidad y la seguridad asociados con usos de datos personales y mantener salvaguardas razonables para controlar riesgos como la pérdida, acceso no autorizado, uso, destrucción o modificación y la divulgación indebida); 5) *acceso y exactitud*: los consumidores tienen derecho a acceder a los datos personales correctos en formatos reutilizables, de una manera que sea apropiada a la sensibilidad de los datos y al riesgo de consecuencias adversas para los consumidores si los datos son inexactos; 6) *accountability*: los consumidores tienen derecho a que los datos personales sean tratados por las empresas con las medidas adecuadas para asegurarse de que se adhieren a la Ley en vigor.

El pasado 9 de febrero de 2016 la Casa Blanca, a través de una Executive Order del Presidente Barack Obama[26], ha constituido el «Federal Privacy Council» en los siguientes términos: *«There is hereby established the Federal Privacy Council (Privacy Council) as the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf. The establishment of the Privacy Council will help Senior Agency Officials for Privacy at agencies better coordinate and collaborate, educate the Federal workforce, and exchange best practices. The activities of the Privacy Council will reinforce the essential work that agency privacy officials undertake every day to protect privacy»*.

[26] Cfr. The White House. Executive Order - Establishment of the Federal Privacy Council (2016). Executive Orders. Recuperado a partir de https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

El *Consejo de privacidad*, similar a las Autoridades de Control establecidas por la regulación europea, tendrá como principales funciones desarrollar recomendaciones para la Oficina de Administración y Presupuesto sobre las políticas de privacidad del Gobierno Federal y los requisitos; coordinar y compartir ideas, mejores prácticas y enfoques para la protección de la privacidad y la aplicación de las salvaguardias adecuadas de privacidad; evaluar y recomendar la mejor manera de abordar la contratación, la formación y las necesidades de desarrollo profesional del Gobierno Federal con respecto a las cuestiones de privacidad; y realizar otras funciones relacionadas con la privacidad, de conformidad con la ley, según lo señalado por el Presidente.

3. Principales reformas del Reglamento General de protección de datos (2015).

El 18 de diciembre de 2015, el Comité de Representantes Permanentes (Coreper) confirmó los textos transaccionales acordados con el Parlamento Europeo sobre la reforma de la protección de datos, después de que el Consejo, el Parlamento y la Comisión alcanzaran un acuerdo final el 15 de diciembre de 2015. Posteriormente, el 14 de abril de 2016 el Parlamento Europeo ha aprobado el texto consensuado. Esta aprobación parlamentaria pone fin a más de cuatro años de trabajo para reformar drásticamente la normativa comunitaria sobre protección de datos. Sin duda, el objetivo del nuevo reglamento general es dar más control a los ciudadanos sobre su información privada en un mundo de teléfonos inteligentes, redes sociales, banca por internet y transferencias globales.

El 25 de mayo de 2015 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[27].

Como han destacado las autoridades europeas, *«es un acuerdo fundamental con consecuencias importantes. Esta reforma no solo refuerza los derechos de los ciudadanos, sino también adapta a la era digital la normativa para las empresas, al tiempo que reduce la carga administrativa. Se trata de textos ambiciosos y con visión de futuro. Podemos tener plena confianza en el resultado»*[28].

La protección de las personas en relación con el tratamiento de sus datos personales es un derecho fundamental consagrado en la Carta de los Derechos Fundamentales de la UE (artículo 8) y en el Tratado de Funcionamiento de la Unión Europea (artículo 16).

El RGPD tiene por objeto mejorar el nivel de protección de los datos de las personas físicas cuyos datos personales se someten a operaciones y procesamiento automatizado o no y aumentar las oportunidades de negocio y libertad de movimiento en el mercado único digital, en particular mediante la reducción de la burocracia administrativa.

En este sentido, cabe destacar los datos que el Consejo Europeo ha tenido en consideración al abordar esta importante reforma[29]: el 57 % de los europeos considera que la divulgación de información personal es una cuestión importante; al 70 % le preocupa que las empresas puedan utilizar la información para fines diferentes de aquellos para los que se ha recogido; solo el 15 % considera que controla completamente la información que aporta en línea; y el 90 % de los europeos cree que es importante que en todos los países de la UE se tengan los mismos derechos y la misma protección.

---

[27] OJ L 119, 4.5.2016, p. 1–88.

[28] Cfr. Consejo de la Unión Europea, Reforma de la protección de datos: http://www.consilium.europa.eu/es/policies/data-protection-reform/

[29] Cfr. European Commission. (2015). *Special Eurobarometer 431. "Data protection"*. Recuperado a partir de http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.

3.1. Nivel de protección de los datos.

Los principios y normas sobre el tratamiento de los datos personales de las personas físicas se fundamentan en el respeto de los derechos y libertades fundamentales, en particular del derecho a la protección de los datos de carácter personal. Este derecho ha sido reforzado con la finalidad de proteger a las personas físicas cuyos datos se someten a procesamiento y asegurar en la práctica un mayor control sobre sus datos personales.

En consecuencia, el Reglamento General se rige por las siguientes directrices:

- Incluye normas más específicas que permiten a los responsables y encargados del tratamiento procesar datos de carácter personal, en particular mediante la exigencia del consentimiento de las personas físicas afectadas u otros títulos jurídicos habilitantes, como la existencia de disposición legal o de relación contractual.
- La mejora de la información sobre el uso y destino específico de los datos personales cuando se comparten, en particular la información a las personas físicas mediante las políticas de privacidad en un lenguaje claro y sencillo o a través de iconos normalizados[30].
- El tratamiento de los datos personales relativos a niños menores de 16 años o, en caso de que el Derecho de un Estado miembro disponga una edad menor, pero en ningún caso inferior a los 13 años, sólo será lícito si dicho consentimiento ha sido dado o autorizado por el titular de la autoridad parental sobre el niño.
- Se regula la información que deberá facilitarse cuando los datos no hayan sido directamente obtenidos del interesado.
- Derecho de acceso más fácil a los datos personales de los interesados.
- El derecho a oponerse por motivos relacionados con la situación particular del interesado al tratamiento de datos personales relacionado con el interés público o con los intereses legítimos del responsable del tratamiento. Este derecho incluye el uso de datos de carácter personal a efectos de la «elaboración de perfiles».
- El derecho «al olvido» (supresión, también en el sentido de «desindexación»[31]) de los datos personales y, que permite, por ejemplo, que los interesados exijan la supresión, sin demora, de datos personales recogidos o publicados en una red social o en un motor de búsqueda.

[30] Entre otras propuestas, resulta de interés el proyecto de iconos normalizados creados por https://disconnect.me/icons. Según explican en su sitio web, su misión es: «*At Disconnect our mission is to make the Internet better by giving people greater transparency and control over the personal information they share online. We do what we do to make it easier for people to protect their privacy and enjoy the Internet*».

[31] El "derecho al olvido" aplicado a los motores de búsqueda comporta la supresión y bloqueo de contenidos de los índice de resultados de buscadores de internet. Tras la Sentencia C-131/12 del Tribunal de Justicia de la UE, dictada el 13 de mayo de 2014 en el asunto Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, se considera que los motores de búsqueda realizan tratamiento de datos personales y, por tanto, han de asumir la responsabilidad que dicho tratamiento implica. Así, cuando dirijan sus servicios a consumidores europeos deben cumplir con la normativa comunitaria vigente y, en consecuencia, atender, estudiar y resolver aquellas solicitudes de ejercicio del derecho de cancelación y oposición al tratamiento de datos en los casos en los que la información haya quedado obsoleta y no exista interés público en acceder a ella.
La aplicación práctica de esta sentencia exige a los buscadores ser capaces hallar el equilibrio entre los derechos del titular de tales datos y el interés legítimo del público general a acceder a dicha información. Esta ponderación habrá de basarse principalmente en cuatro factores: 1) la naturaleza de la información de que se trate, así sea inexacta o falsa, incompleta o inadecuada, excesiva, obsoleta o ya no relevante; 2) el carácter sensible de esta información para la vida privada del individuo; 3) el interés público en disponer de dicha información en el presente; y 4) el papel que dicha persona desempeñe en la vida pública.
La solicitud entonces puede ser dirigida directamente al responsable del motor de búsqueda con independencia de que los datos sean o no eliminados de la página web donde fueron publicados y será este quien deberá decidir, caso por caso, acerca de la idoneidad de la solicitud del particular atendiendo siempre a la concurrencia de factores indicados anteriormente. En caso de que el usuario no esté conforme con la respuesta del buscador siempre podrá solicitar la tutela de la agencia de protección de datos o tribunales de su jurisdicción para que resuelva si es legítima su solicitud.

- El derecho a la portabilidad debe facilitar la transmisión de datos personales de un proveedor de servicios, como una red social, a otro en un formato estructurado y de uso habitual y de lectura mecánica. Este derecho aumentará los derechos en materia de protección de datos y también mejorará la competencia efectiva entre proveedores de servicios.
- Obligación de notificación relativa a la rectificación, supresión o limitación a cada uno de los destinatarios a los que se hayan comunicado los datos, salvo que ello sea imposible o exija un esfuerzo desproporcionado. El responsable del tratamiento informará al interesado acerca de estos destinatarios, si el interesado así lo solicitara.
- Salvaguardias comunes que afectan al tratamiento de datos personales con fines de archivo por razones de interés público o para fines de investigación científica e histórica o estadísticos.
- Derecho a presentar una reclamación ante una autoridad de control y derecho a un recurso judicial efectivo contra una autoridad de control por tribunales nacionales, con independencia del Estado miembro en que esté establecido el responsable del tratamiento.

3.2. «Mercado único digital».

El Reglamento General establece una normativa única, válida en toda la UE y aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

En un entorno globalizado como el tecnológico, la aplicación extraterritorial de las normas constituye un verdadero desafío, pues no tendría demasiado sentido limitarlas a un determinado espacio, por el principio de aplicación territorial de la Ley, o a un concreto conjunto de personas, por imperativo del principio de personalidad.

De este modo, el Reglamento General incorpora nuevas reglas sobre extraterritorialidad de las normas y se aplicará fuera de la Unión Europea cuando el tratamiento de datos personales de interesados residentes en la Unión se efectúe por responsables o encargados del tratamiento no establecidos en la Unión y las actividades de tratamiento estén relacionadas con dos ámbitos: *a)* la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte del interesado; o *b)* el control de su conducta, en la medida en que esta tenga lugar en la Unión Europea.

Asimismo, el Reglamento se aplicará extraterritorialmente al procesamiento de datos personales realizados por responsables del tratamiento no establecidos en la Unión pero a los que sea aplicable la legislación nacional de un Estado miembro en virtud del Derecho internacional público, por ejemplo, en razón de la ciudadanía o residencia comunitaria o por aplicación de normas diplomáticas.

Se evita así una situación en la que unas normas nacionales contradictorias en materia de protección de datos podrían alterar el intercambio transfronterizo de datos.

Igualmente prevé el refuerzo de la cooperación entre los Estados miembros a fin de garantizar la aplicación coherente de las normas de protección de datos en toda la UE. Esto generará una competencia leal y animará a las empresas y entidades, sobre todo a las pequeñas y medianas, a sacar el máximo provecho del mercado único digital (Parlamento Europeo, 2016)[32].

[32] Cfr. Parlamento Europeo. (2016). *El mercado único digital omnipresente*. Recuperado 26 de febrero de 2016, a partir de http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.9.4.html.
El Parlamento Europeo afirma que El mercado único digital es uno de los ámbitos más prometedores y más desafiantes del progreso, que crea posibilidades de mejora de la eficiencia por valor de 415 000 millones de euros. Abre nuevas oportunidades para fomentar las opciones de negocio mediante el comercio electrónico, a la vez que facilita el cumplimiento de los requisitos administrativos y financieros para las empresas y da capacidades a los

Para reducir costes y crear mayor seguridad jurídica, en los casos transfronterizos importantes en los que intervengan varias autoridades nacionales de control, se adoptará una decisión de control única. Este «mecanismo de ventanilla única» permite que una entidad establecida en varios Estados miembros se relacione únicamente con la autoridad de protección de datos del Estado miembro de su establecimiento principal, y no con tantas autoridades como Estados en los que pueda estar establecida[33]. Ese mecanismo prevé asimismo una decisión única aplicable a todo el territorio de la UE en caso de disputas.

De otra parte, el Reglamento se fundamenta en un enfoque dirigido a los riesgos, con objeto de reducir los costes administrativos: los responsables del tratamiento pueden poner en práctica medidas según el riesgo que impliquen las operaciones de tratamiento de datos practicadas. Las entidades pueden realizar diversas actividades las cuales pueden comportar riesgos para la intimidad y la privacidad, riesgos que además pueden variar: desde el uso ilícito de datos por carecer del necesario consentimiento expreso hasta la divulgación excesiva de datos personales en Internet, además de posibles cesiones de información personal a entidades o personas con las que el responsable del tratamiento esté vinculado. El RGPD no ofrece una solución única válida para todos los casos: cuantos mayores riesgos supongan las actividades para los datos personales, más estrictas serán las obligaciones.

Por esta razón, las obligaciones jurídicas del responsable del tratamiento vendrán determinadas en función de la naturaleza, el ámbito, el contexto y los fines del procesamiento de datos, así como por los riesgos existentes, de diversa probabilidad y gravedad, para los derechos y libertades de las personas físicas. Por consiguiente, el responsable del tratamiento deberá aplicar aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales es llevado a cabo de conformidad con el Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Igualmente se establece la «evaluación de impacto relativa a la protección de datos» cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas. Por ejemplo, en el ámbito de instituciones que procesen datos sensibles, como los de salud, religión, creencias, datos de menores o de afiliación política o sindical, se deberá evaluar el sistema para asegurar el cumplimiento y correcta implementación de las medidas técnicas y organizativas necesarias para garantizar la protección de los derechos de los titulares de la información, en especial en los supuestos de comunicaciones o cesiones de datos a otras entidades o terceros.

3.3. Mejora de instrumentos para garantizar la protección de datos.

El Reglamento establece una serie de medidas para aumentar la responsabilidad y la rendición de cuentas de los responsables del tratamiento a fin de garantizar el pleno cumplimiento de las nuevas normas de protección de datos.

---

clientes a través de la administración electrónica (e-government). Los servicios del mercado y de la administración desarrollados dentro del mercado único digital están evolucionando de plataformas fijas a plataformas móviles, son cada vez más omnipresentes y ofrecen acceso a la información y al contenido en cualquier momento, lugar o dispositivo (comercio omnipresente y administración omnipresente). Estos avances requieren un marco normativo que facilite el desarrollo de la computación en nube, una conectividad de datos móviles sin fronteras y un acceso simplificado a la información y al contenido, preservando la privacidad, los datos personales, la seguridad cibernética y la neutralidad de la red.
El fundamento jurídico del mercado único digital se encuentra en los artículos 4, apartado 2, letra a), 26, 27, 114 y 115 del Tratado de Funcionamiento de la Unión Europea (TFUE).

[33] El art. 51.bis.1 RGPD regula la competencia de la autoridad de control principal y dispone que *«sin perjuicio de lo dispuesto en el artículo 51, la autoridad de control del establecimiento principal o del único establecimiento del responsable del tratamiento o del encargado será competente para actuar como autoridad de control principal para el tratamiento transfronterizo por parte de este responsable o este encargado del tratamiento»*.

Uno de los temas más polémicos ha sido la adjetivación del consentimiento como "explícito" contenida en la propuesta de la Comisión Europea, aunque finalmente la redacción ha vuelto a la calificación de "inequívoco" ya presente en la Directiva, con el fin de asegurar en todo caso su expresión mediante una manifestación o una clara acción afirmativa.

Asimismo, los responsables del tratamiento deben poner en práctica una serie de medidas de seguridad, incluida la obligación de notificar las violaciones de datos personales en determinados casos. Para que la efectividad de las normas contenidas en el Reglamento resistan el paso del tiempo y la permanente innovación tecnológica, se introducen los principios de protección de datos «desde el diseño y por defecto», de tal manera que el responsable del tratamiento cumpla los requisitos del Reglamento y se protejan realmente los derechos de los interesados desde la planificación de los proyectos («desde el diseño») y en todo caso («por defecto»).

Entre las medidas particulares que contempla el Reglamento General, destaca que el responsable y el encargado del tratamiento estarán obligados a designar un «delegado de protección de datos» para garantizar el cumplimiento de la normativa en ciertos supuestos[34].

Los interesados y, en determinadas condiciones, las organizaciones de protección de datos podrán presentar reclamaciones ante una autoridad de control o interponer un recurso en caso de que no se cumplan las normas de protección de datos.

En caso de infracción de la normativa establecida, los responsables del tratamiento pueden enfrentarse a multas de hasta 20.000.000 de euros o el 4 % de su volumen de negocios anual mundial, por incumplimiento de las resoluciones de la autoridad de control.

3.4. Privacidad de la geoinformación.

3.4.1. Nuevo marco global de la privacidad.

En la actualidad se llevan a cabo diversas iniciativas legislativas para la regulación de la privacidad en numerosos países del mundo, además de en Estados Unidos y Europa. Estas reformas tienen un enorme calado para la legislación futura e incluyen nuevas reglas legales, principios de neutralidad tecnológica y una regulación estable para entornos digitalizados y de procesamiento masivo y transfronterizo de información personal.

La actual revisión de instrumentos internacionales en privacidad alcanza a todos los niveles de gobierno y organización, tanto internacionales como nacionales. Con carácter general, los principios fundamentales que rigen hasta el momento se circunscriben a la interoperabilidad y a la compatibilidad de los sistemas internacionales de protección.

En este sentido, el marco global de la privacidad en la geoinformación también queda delimitado por los principios de toda sociedad democrática y respetuosa con los derechos fundamentales, pues sin la privacidad no habría respeto a la dignidad ni a la libertad de las personas.

3.4.2. Tecnología geoespacial y Derecho.

Tecnología y Derecho son realidades que han de armonizarse en el ámbito de la geoinformación para una mayor expansión digital. El Derecho debe asumir la realidad digital para garantizar su crecimiento y aumentar las ventajas personales, sociales y económicas. Sin embargo, el Derecho se enfrenta a importantes desafíos digitales. Los instrumentos y las aplicaciones tecnológicas crean nuevos riesgos para la seguridad personal de las personas y, en un contexto más amplio, para la seguridad nacional en cuyo seno ha de desenvolverse la libertad de las personas. En este contexto, el derecho fundamental a la protección de datos desempeña una función esencial para la protección de las personas y sus datos, así como para la configuración del ejercicio de los derechos en las democracias y estados modernos.

[34] Cfr. art. 35 y ss. RGPD.

El importante desarrollo tecnológico permite a las personas de forma universal utilizar las tecnologías de la información y las comunicaciones, aunque incrementa la capacidad de vigilancia, interceptación y recopilación de datos por parte de gobiernos, empresas y personas, con la consiguiente violación o transgresión de los derechos humanos y, en particular, del derecho a la privacidad.

Por ello, en el ámbito de los datos y servicios geoespaciales hay que reafirmar el derecho humano a la privacidad, pues nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia. En el ámbito de su ejercicio es importante el respeto al derecho a la libertad de expresión, de información y de libre opinión.

3.4.3. Privacidad y seguridad.

En el equilibrio entre privacidad y seguridad, ámbitos donde la geoinformación desempeña una función crítica o estratégica, los Estados deben garantizar el pleno cumplimiento de sus obligaciones en virtud del derecho internacional de los derechos humanos.

El ámbito de la seguridad nacional cobra una importancia creciente y ha de tener en cuenta las implicaciones que el uso de los datos y servicios espaciales tiene en cada Estado. Es necesaria una mayor tarea de armonización de criterios y legislaciones, pues algunas lagunas legislativas o ausencias de homogeneización generan conflictos entre Estados y regiones que difunden su geoinformación y crean desigualdades en los Estados que no publican o distribuyen geoinformación de manera interoperable.

3.4.4. Privacidad de la geoinformación.

Actualmente existen numerosas iniciativas legislativas, tanto internacionales y transnacionales, como nacionales y regionales. Desde Estados Unidos de América hasta Europa, pasando por Asia y Pacífico, existe una preocupación creciente para reconocer normativamente el derecho fundamental y autónomo a la protección de datos de carácter personal.

Junto a esas numerosas propuestas, también existe un interés cada vez mayor en la regulación de la privacidad en el ámbito de la geoinformación, por su importancia, mayor difusión de infraestructuras de datos espaciales y su valor geoestratégico para la seguridad y defensa nacional, y también para la administración electrónica, empresas y ciudadanos.

La geolocalización ha experimentado un desarrollo exponencial en los últimos años. Su expansión ha sido más técnica que jurídica, y muchas de las normas sobre privacidad o protección de datos no han prestado una atención específica al impacto de la ubicación geográfica, aunque muchas mencionan la cartografía o la geografía como aspectos relevantes a tener en cuenta.

En la actualidad no hay duda de que la información geográfica ejerce un papel importante en la sociedad. Casi todas las decisiones humanas, y las realidades sociales y económicas, tienen un componente geográfico. En general, el valor de la información aumenta cuando está conectado a una ubicación. Todos los tipos de información se pueden conectar a una ubicación geográfica, tales como datos financieros, los datos de salud y otros datos de comportamiento de los consumidores. Con el rápido desarrollo tecnológico y la amplia adopción de dispositivos móviles inteligentes, se está desarrollando una nueva categoría de servicios basados en la localización.

La gestión de la geoinformación comprende en la actualidad muy diversos aspectos y en la actualidad es un hecho que la tecnología geoespacial se ha generalizado e internacionalizado. Esta premisa permite comprender el alcance e impacto que las diversas tecnologías tienen en la privacidad de la geolocalización.

En el ámbito de la geolocalización consideramos más adecuado adoptar un concepto amplio de datos personales que un concepto restringido que impida la protección efectiva de los datos que afectan a la persona.

Un concepto amplio de datos personales no significa que esa noción resulte ilimitada. La finalidad de las disposiciones normativas es proteger los derechos y las libertades fundamentales individuales, en especial el derecho a la intimidad y a la privacidad, considerados como derechos autónomos, en lo que se refiere al tratamiento de datos personales. En consecuencia, las normas en esta materia se concibieron para aplicarse en situaciones en que los derechos individuales pueden estar en peligro y, por tanto, necesitar protección. De igual manera, el ámbito objetivo de aplicación de las normas de protección de datos debe definirse con precisión, sin excesiva amplitud pero sin permitir una limitación indebida del concepto objetivo de datos personales.

La generación, almacenamiento y distribución de la geoinformación requiere la intervención de numerosos agentes en los diversos aspectos de una amplia cadena de producción no sólo de los datos espaciales, sino también de sus metadatos y de sus servicios asociados en línea y fuera de línea. El impacto que la producción cartográfica puede tener en la privacidad no es pequeño y requiere considerar la responsabilidad efectiva de cada faceta. Ciertamente, la complejidad de los procesos de tratamiento junto a la diversidad de administraciones, corporaciones, empresas y profesionales implicados requiere delimitar su respectiva responsabilidad específica.

3.4.5. Interoperabilidad jurídica de la geoinformación.

La interoperabilidad de los datos y servicios espaciales en sus dimensiones técnica, semántica, organizativa y jurídica es esencial para el progreso de la sociedad al permitir el conocimiento del espacio terrestre, marino y aéreo, generando valor añadido y estratégico en las actividades y sectores que precisan esa información.

La *interoperabilidad jurídica* es la dimensión de la interoperabilidad relativa a la relación e interacción entre los agentes jurídicos y operadores técnicos implicados en actuaciones, procesos y procedimientos administrativos, judiciales o extrajudiciales que, con soporte en sistemas de información interpretable de forma automática y reutilizable por aplicaciones, comparten datos y servicios integrados, accesibles, fiables y sostenibles en el tiempo, e intercambian conocimientos para el objeto específico requerido por su actividad.

La interoperabilidad jurídica de la geoinformación facilita conocer las implicaciones jurídicas y tecnológicas que surgen en relación al espacio en todos los niveles, en la sociedad en general, en el desarrollo comercial e industrial, y en las relaciones particulares, sociales y económicas de ciudadanos y empresas.

Un buen nivel de servicio y una sólida arquitectura tecnológica favorece que la información geoespacial disponible resulte efectiva y eficiente en la práctica, también en el ámbito jurídico, administrativo y judicial, y asegura el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados por medios electrónicos y en red.

El ámbito de la interoperabilidad jurídica alcanza a 1) la coordinación de los datos y el intercambio de servicio, 2) los acuerdos jurídicos marco, 3) la transparencia en los datos, 4) las licencias, 5) los mecanismos de cobro o acceso público, 6) los usos de emergencia y 7) los datos de terceros.

3.4.6. Políticas de difusión de datos y servicios.

El éxito y buen fin de las políticas de difusión de datos y servicios habría de considerar algunos criterios y aspectos decisivos: 1) minimizar los obstáculos para el uso de información geoespacial; 2) optimizar la armonización de las licencias; 3) reducir esfuerzos para aplicar correctamente las licencias; 4) clarificar los procesos para tomar decisiones sobre el propio

acuerdo y 5) prever el modo de intercambio de la geoinformación, incluso mediante plataformas o infraestructuras.

Una política de licencias bien definida es importante para desarrollar acuerdos claros y sistemáticamente estructurados, así como para establecer procedimientos sencillos y operativos y revisarlos cuando resulte necesario.

3.5. Garantías para la transferencia de datos personales al exterior de la UE.

El Reglamento General contiene normas para la transferencia de datos personales a terceros países y organizaciones internacionales. Las transferencias pueden llevarse a cabo siempre que se cumpla una serie de condiciones y salvaguardias, en particular cuando la Comisión haya decidido que existe un *nivel adecuado de protección*.

Las nuevas decisiones sobre el carácter "adecuado" de la protección tendrán que revisarse al menos cada cuatro años. Las autorizaciones y decisiones existentes sobre esa "adecuación" seguirán en vigor hasta que se modifiquen, sustituyan o deroguen. En definitiva, el Reglamento introduce un mecanismo vinculante de actualización periódica para evitar que la evolución tecnológica haga inútiles las garantías legales y deje a los ciudadanos desprotegidos *de facto* en sus derechos.

El principio general de las transferencias determina que únicamente podrán realizarse transferencias de datos personales que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional si el responsable y el encargado del tratamiento cumplen las condiciones establecidas por la norma, en particular sobre las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Así, por ejemplo, no será suficiente para autorizar una transferencia de un servicio de alojamiento de documentos en la nube que el proveedor afirme ser seguro, sino que se precisará que acredite que ha implementado las medidas de seguridad oportunas y que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también éstos adoptan las garantías tecnológicas suficientes.

El espíritu y finalidad del Reglamento quieren garantizar que sus normas ofrecen el máximo nivel de protección de los particulares, de modo que en la práctica se impida su incumplimiento o menoscabo a través de conductas que distorsionen o desfiguren el régimen protector de las transferencias internacionales de datos.

Por ello, el nuevo régimen de transferencias no se limita sólo a regular las transferencias con una decisión de suficiencia, sino que también incluye normas claras para posibilitar transferencias mediante garantías apropiadas, transferencias mediante normas corporativas vinculantes y contempla significativas excepciones para dar viabilidad práctica a situaciones específicas.

3.6. Principios.

El Reglamento General formula y actualiza los principios relativos al tratamiento de datos personales en los siguientes términos, pues los datos personales deberán ser:

a) tratados de manera lícita, leal y transparente en relación con el interesado («*licitud, lealtad y transparencia*»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; todo nuevo tratamiento de los datos personales en interés público o con fines investigación científica e histórica o estadísticos, se efectuará con arreglo al artículo 83, apartado 1, y será considerado compatible con los fines iniciales («*limitación de la finalidad*»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («*minimización de datos*»);

d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin demora los datos personales que sean inexactos con respecto a los fines para los que se tratan («*exactitud*»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines por los que se tratan los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que los datos se archiven exclusivamente en interés público o con fines de investigación científica e histórica o estadísticos, de conformidad con el artículo 83, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas adecuadas que impone el Reglamento a fin de proteger los derechos y libertades del interesado («*limitación del plazo de conservación*»);

f) tratados de tal manera que se asegure una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales mediante la aplicación de medidas técnicas u organizativas adecuadas («*integridad y confidencialidad*»); y

g) el responsable del tratamiento será responsable y capaz de demostrar el cumplimiento normativo («*rendición de cuentas*»).

3.7. Derechos de los interesados.

El Reglamento General se inspira en la protección real y efectiva de los datos personales y comprende un conjunto armonizado de derechos, no sólo al reconocer los ya existentes en normas internacionales y nacionales como los de acceso, rectificación, cancelación y oposición, sino también al configurar dos nuevos derechos: el «olvido digital», también denominado supresión (art. 17 RGPD) y la «portabilidad de datos» (art. 18 RGPD).

3.7.1. Derecho al olvido.

La nueva configuración del Derecho al Olvido[35] viene recogida en el artículo 17 del Reglamento General y se configura por vez primera como un derecho autónomo a los denominados «derechos ARCO» (acceso, rectificación, cancelación y oposición).

3.7.1.1. La Jurisprudencia europea precedente al Reglamento General.

Al comienzo de este estudio hemos expuesto con detalle la situación del proceso legislativo seguido para aprobar la *Propuesta de Reglamento 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*.

El interés de esta norma no reside sólo en su contenido, aun cuando es de enorme importancia, sino también en el momento temporal en que se plantea. Su coincidencia temporal en el Parlamento Europeo con la cuestión prejudicial de interpretación del "derecho al olvido" ante el TJUE ha dado lugar a una situación ciertamente singular e histórica.

[35] Existen diversos estudios sobre la cuestión. Cabe destacar algunos de los más significativos: Martínez Martínez, R. (2014). Aplicar el derecho al olvido. *Revista Aranzadi de derecho y nuevas tecnologías*. Editorial Aranzadi. Recuperado a partir de https://dialnet.unirioja.es/servlet/articulo?codigo=4917063; Moya Izquierdo, S., & Crespo Vitorique, I. (2014). *Los motores de búsqueda y el "derecho al olvido" cuando la tecnología avanza más rápido que el Derecho*. *Unión Europea Aranzadi*. Editorial Aranzadi. Recuperado a partir de https://dialnet.unirioja.es/servlet/articulo?codigo=5052233&info=resumen&idioma=ENG; Paños Pérez, A. (2012). Conflict between freedoms of expression and information and the right of honour, privacy and self-image of minors. *Revista de Derecho*. Facultad de Ciencias Jurídicas y Sociales. Recuperado a partir de https://dialnet.unirioja.es/servlet/articulo?codigo=5333364&info=resumen&idioma=ENG y Rallo Lombarte, A., & Díaz Díaz, E. (2014). Caso Google vs. España: sentencia del TJUE 13 de mayo de 2014. *Actualidad jurídica Aranzadi*, (886), 8. Recuperado a partir de http://ezproxy.si.unav.es:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url&db=edsdnp&AN=edsdnp.4863051ART&lang=es&site=eds-live.

Los poderes legislativo y judicial europeos se han encontrado a la vez, desde los años 2011 y 2012, con el debate y el estudio de tan importante derecho de los ciudadanos europeos. De alguna manera, las decisiones adoptadas en sede judicial (TJUE) han ido marcando la pauta del debate europarlamentario.

La Vicepresidenta de la Comisión Europea y Comisaria Europea de Justicia, Derechos Fundamentales y Ciudadanía en 2012, Viviane Reding, propuso la aprobación del Reglamento General de protección de datos e impulsó la reforma para proteger mejor los datos de los ciudadanos que circulan en Internet y el "derecho al olvido" de los datos que las personas "cuelgan" en Internet.

Con el fin de adaptarse a las exigencias del Tratado de Lisboa, la propuesta de la Comisión Europea comporta un nuevo marco legislativo europeo de protección de datos personales, cuyo eje es que los ciudadanos tienen derecho a ejercer un control efectivo sobre la información personal que les concierne[36].

Según sus propias palabras, *"en Europa tenemos varios derechos: derecho a libertad de prensa o de Internet, si quiere: a la información; derecho a la privacidad y derecho de propiedad intelectual. Ninguno es absoluto. Tiene que equilibrarse con los demás. Los derechos de protección de datos de los periodistas están fuera de esta ecuación porque necesitan recolectar datos para hacer información. Que es distinto a que yo quiera que mis datos personales estén protegidos y tenga derecho a recuperarlos de donde estén. No puedo cambiar una historia o la Historia ni intervenir en un poema o pintura, tampoco en los archivos de un periódico"*[37].

Con anterioridad, la Vicepresidenta Reding había expuesto[38] que los derechos de las personas habrían de construirse sobre pilares fundamentals, entre los que destacaba como primero y básico el *"right to be forgotten": a comprehensive set of existing and new rules to better cope with privacy risks online".* Estas nuevas reglas, para lograr una verdadera modernización de la legislación, incluyen expresamente el derecho - y no sólo la "posibilidad"- de las personas para retirar su consentimiento al procesamiento de datos. En este sentido, como sostenía la Vicepresidenta de la Comisión Europea, *"la carga de la prueba debe estar en los controladores de datos, los que procesan sus datos personales. Ellos deben demostrar que necesitan para mantener los datos en lugar de los individuos tener que probar que la recogida de sus datos no es necesaria"*.

De esta manera, la cuestión prejudicial de interpretación se ha fundamentado y referido directamente a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[39], si bien ha sido crucial entre las deliberaciones parlamentarias, donde incluso en la última propuesta, como ya hemos expuesto, el denominado *"right to be forgotten"*, "derecho al olvido", adopta la más precisa denominación de *"right to erasure"*, "Derecho a la supresión".

---

[36] Cfr. Blume, P. (2012). Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*, *2*(3), 130-136. http://idpl.oxfordjournals.org/content/early/2012/04/14/idpl.ips007.

[37] Cfr. El País Digital, *"Viviane Reding: Quien pone datos personales en la Red tiene derecho a recuperarlos"*, 25/01/2012, accesible en: http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id=51316.

[38] Cfr. SPEECH/11/183, Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, *Your data, your rights: Safeguarding your privacy in a connected world*, Privacy Platform "The Review of the EU Data Protection Framework", Brussels, 16 March 2011. Accesible en: http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm?locale=en. *"Peoples' rights need to be built on four pillars: The first is the "right to be forgotten": a comprehensive set of existing and new rules to better cope with privacy risks online. When modernising the legislation, I want to explicitly clarify that people shall have the right – and not only the "possibility" – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary (...)"*.

[39] Diario Oficial n° L 281 de 23/11/1995 p. 0031 - 0050.

Una vez dictada la Sentencia del Tribunal de Justicia (Gran Sala), de 13 de mayo de 2014, en los términos antes expuestos, la Audiencia Nacional de España procedió a levantar la suspensión de los procesos incoados por Google Spain, S.L., y Google, Inc..

Recibida en España la Sentencia del TJUE, la Audiencia Nacional dio traslado a las partes en el proceso para que hicieran alegaciones y, en algún caso, para que además se pronunciaran sobre el mantenimiento de las pruebas admitidas pero no remitidas en plazo por Google.

Terminada la fase de alegaciones de las partes en el procedimiento sobre la incidencia de la Sentencia dictada por el TJUE, las actuaciones quedaron pendientes para votación y fallo, lo cual tuvo lugar en el mes de noviembre de 2014, concluyéndose la deliberación el 18 de diciembre 2014, tras la cual la Audiencia Nacional dictó la Sentencia de 29 de diciembre de 2014.

Con anterioridad y paralelamente al proceso del caso enjuiciado por el TJUE, según se ha sabido con posterioridad, Google Spain, S.L., y Google, Inc., solicitaron el *desistimiento de la acción ejercitada* en cuanto los autos quedaron vistos para sentencia, conforme al art. 74.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. Estas solicitudes de desistimiento han sido admitidas, previas las actuaciones pertinentes, y han afectado a más de 130 asuntos[40].

3.7.1.2. Conceptos de «bloqueo» y de «supresión».

El RGPD define el «olvido digital» como el *«derecho a obtener del responsable del tratamiento la supresión de los datos personales que le conciernan sin demora injustificada, y el responsable del tratamiento tendrá la obligación de suprimir los datos personales sin demora injustificada cuando concurra alguna de las circunstancias»* que expresamente regula el artículo 17 del RGPD.

Por tanto, es esencial diferenciar con claridad los diversos conceptos. Como han señalado algunos autores en relación con el concepto de «bloqueo» y de «supresión» en el ámbito español —citado por ser de los más innovadores—, *«el proyecto del Reglamento [español] incluía en su versión sometida a trámite de información pública dos definiciones referidas a los mencionados efectos de bloqueo y supresión. Así, se definía bloqueo como «la identificación y reserva de datos de carácter personal con el fin de impedir su tratamiento excepto por parte de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. (…) Por su parte, la supresión era definida como «la eliminación física de los datos de carácter personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento durante el cual se guardaron bloqueados»*[41].

Sin embargo, en el texto legal definitivo sendas definiciones fueron suprimidas por su falta de claridad y se han reemplazado por un concepto nuevo: "cancelación". El art. 5.1.b) RLOPD define cancelación en estos términos, incluyendo bloqueo y, en su caso, supresión: *Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.*

---

[40] Cfr. *Google desiste en 136 casos sobre el 'derecho al olvido' recurridos ante la Audiencia Nacional*, EUROPA PRESS, Publicado 23/01/2015. Accesible en: http://www.europapress.es/sociedad/noticia-google-desiste-136-casos-derecho-olvido-recurridos-audiencia-nacional-20150123193520.html

[41] Cfr. Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre). Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, SA, Diciembre de 2008.

A nuestro juicio, este aspecto es muy relevante en el análisis del derecho al olvido, a pesar de que no se le ha dado toda la importancia real que comporta. Como indica la magistrada de la Audiencia Nacional BUISÁN GARCÍA, *«el bloqueo llevará aparejado que los datos se encierren, aíslen o incomuniquen, de tal manera que resulte imposible su ulterior tratamiento o utilización, salvo en los supuestos indicados»*. Por consiguiente, la diferenciación entre bloqueo y supresión tiene una enorme aplicación práctica en el ámbito de la desindexación de los motores de búsqueda[42].

Autores como DAVARA RODRÍGUEZ han señalado *que «la cancelación no es lo mismo que el borrado; la cancelación no puede exigir el borrado total y absoluto de los datos, aunque sea necesario el bloqueo con todas las características de seguridad que le deban acompañar»*[43].

La Agencia Española de Protección de Datos (AEPD) ha precisado[44] que *el ejercicio de estos derechos [de rectificación o cancelación] supone el cese en el tratamiento y uso de los datos personales del solicitante por parte del responsable del fichero al que se dirige la solicitud de cancelación, y conlleva el bloqueo de sus datos personales por la entidad titular del fichero e impide el tratamiento de los mismos con fines promocionales.*

El bloqueo ha de ser considerado como la reserva de los datos necesaria para atender, en su caso, a las posibles responsabilidades derivadas del tratamiento o de la relación subyacente al mismo, de manera que deberá ser posible a la autoridad judicial o administrativa acceder al dato previamente sometido a tratamiento y poder valorar efectivamente las posibles responsabilidades exigidas por el afectado o por la propia autoridad judicial o administrativa.

El dato deberá conservarse bloqueado en los supuestos en que la cancelación procede de la propia solicitud del afectado así como cuando se haya producido de oficio por el responsable, ante la inexactitud o ilicitud del tratamiento, o bien ante el cumplimiento de la finalidad que justificaba el tratamiento.

La AEPD ha analizado la figura del bloqueo en numerosos informes[45] y ha señalado que *«existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado»*.

Durante el bloqueo, los datos quedan disponibles para Jueces, Tribunales y Administraciones Públicas, aunque no es posible su tratamiento «activo». En cuanto al modo de llevarse a cabo el bloqueo, la AEPD concreta[46] que *«deberá efectuarse de forma tal que el acceso a los datos quede limitado en función de las finalidades que amparan la no supresión física de los datos en cuestión. De este modo, pese a permanecer el tratamiento de los datos,*

---

[42] Conviene aclarar la diferencia entre el derecho de cancelación y el derecho de oposición. En palabras de la AEPD, *"El derecho de oposición se configura como un derecho distinto del derecho de cancelación ya que el tratamiento de los datos respecto de los que se solicita la cancelación no podrá ser considerado lícito, bien por haber devenido inadecuado, o por que se vulneran los principios de calidad consagrados en el artículo 4 de la Ley Orgánica 15/1999. Sin embargo, el derecho de oposición opera en los supuestos en los que el tratamiento de datos es plenamente lícito, pero que en razón a la específica situación personal alegada por el afectado procede que se exceptúe su tratamiento. Por consiguiente, el ejercicio del derecho de oposición obliga al responsable del fichero a realizar una valoración de la situación personal del afectado, considerando si procede exceptuar dicho tratamiento"* (Informe Jurídico AEPD 0168/2012).

[43] Cfr. *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal.* Estudios y Comentarios Legislativos (Civitas). Troncoso Reigada, A. Editorial Aranzadi, SA, Junio de 2010.

[44] Resolución: R/00122/2015, Procedimiento Nº PS/00524/2014, 9 febrero 2015.

[45] Cfr. Informe Jurídico AEPD de 1 de agosto de 2007.

[46] Resolución AEPD R/00066/2003.

el acceso a los mismos quedará enteramente restringido, de acuerdo con las finalidades indicadas en las normas anteriores».

Estas cuestiones no constituyen simplemente disquisiciones teóricas, sino que poseen un efectivo interés práctico. Así, el artículo 17 bis, párrafo 2º del RGPD, recogiendo los anteriores conceptos, dispone que *«Cuando el tratamiento de datos personales haya quedado limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o con miras a la protección de los derechos de otra persona física o jurídica o por motivos de interés público importante de la Unión o de un determinado Estado miembro»*.

3.7.1.3. Configuración jurídica del nuevo derecho.

La nueva configuración del *derecho al olvido digital* trasciende el contenido del *derecho de cancelación* en el entorno digital, según se ha venido aplicando en cumplimiento de la Directiva europea de privacidad y de las normas nacionales.

Por ejemplo, el olvido digital supera la necesidad de solicitar al titular de una página web la previa o simultánea eliminación de una determinada información no adecuada y excesiva, para solicitar su posterior desindexación. En consecuencia, como ha reconocido el TJUE en la Sentencia de 13 de mayo de 2014, *«el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita»*[47].

En la práctica, este derecho tiene una dimensión dual: por una parte, para el ciudadano supone un reconocimiento de la pretensión de suprimir de inmediato la información afectada en el sitio web, así como de abstenerse de dar difusión a esta información siempre que el titular de los datos lo solicite. Este derecho podrá ejercitarse por el ciudadano en aquellos casos en que el tratamiento no se ajuste a la normativa, cuando exista oposición por razones personales del interesado o bien se retire el consentimiento al tratamiento, o los datos no sean necesarios para los fines para los que fueran recogidos, o hubiera expirado el plazo de conservación de la información personal.

Si, durante el transcurso del tratamiento de los datos la entidad, corporación, sitio web, red social o, en definitiva, el responsable del tratamiento hubiera hecho públicos los datos, dicho responsable estará en la obligación de adoptar las medidas necesarias, no sólo organizativas, sino también las técnicas oportunas, con el fin de informar a los terceros sobre la solicitud de cancelación del interesado para que supriman sus datos.

De otra parte, también resulta relevante destacar que este derecho incide en la esfera del Responsable del tratamiento, esto es, la entidad, corporación, sitio web o red social que trata los datos. El Responsable del tratamiento deberá optar entre limitar el tratamiento (art. 17 bis RGPD), o bien suprimir sin demora la información (art. 17 RGPD), ponderando caso por caso el alcance de este derecho con el derecho a la libertad de expresión, la salud pública, el deber de conservación de los datos para dar cumplimiento a una obligación legal y el interés público[48].

---

[47] Cfr. Resolución tercera de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014 (C-131/12 - Google Spain y Google) (2014). Recuperado a partir de http://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12.

[48] Para mayor información sobre la aplicación práctica y los criterios de ponderación, cfr. Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/121. WP225. Accesible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

3.7.2. Derecho a la portabilidad de datos.

La portabilidad de los datos es el otro nuevo derecho reconocido en el artículo 18 del RGPD. Atribuye al interesado la facultad de «*recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos*».

Este derecho no ha tenido unos antecedentes jurisprudenciales tan amplios como los del olvido digital y se ha suscitado principalmente por razones de interoperabilidad técnica.

No obstante, el Reglamento General ya prevé que el ejercicio de este derecho se entenderá sin perjuicio del olvido digital y la supresión regulada en el artículo 17. En la práctica habrá de ponderarse el ejercicio de este derecho con los casos de tratamiento necesario para el cumplimiento de misiones de interés público (por ejemplo en el caso de la administración tributaria, geográfica o de justicia) o inherente al ejercicio del poder público conferido al responsable del tratamiento (como podría ocurrir en el ejercicio de competencias expropiatorias o sancionadoras).

A estos dos nuevos derechos cabe añadir la mayor concienciación que existe en materia de privacidad en los entornos en línea, la efectiva aplicación de la «privacidad desde el diseño» (*privacy by design*) en el desarrollo de productos, aplicaciones y soluciones, así como el establecimiento de la obligación para el Responsable del tratamiento de realizar evaluaciones de impacto de la normativa en el tratamiento de datos de carácter personal, incluidos los códigos de conducta.

En definitiva, los instrumentos jurídicos que complementan el ejercicio de los derechos ARCO y de los dos nuevos derechos regulados en el RGPD posibilitarán a los ciudadanos una mayor salvaguarda de su privacidad, pues el titular de los datos dispondrá de mejores garantías para su defensa y protección.

3.8. Menores.

El ámbito de los Menores es uno de los más delicados y agudos de los que se encuentran en la Protección de Datos, y sorprende la atención que se le ha prestado ya desde la nueva Propuesta de Reglamento, no sólo en sede de principios, como por ejemplo en los de calidad de datos y habilitación para el tratamiento, sino también en la regulación contenida en el artículo 8 del RGPD sobre «*condiciones aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información*».

Estas normas pueden aplicarse también de forma análoga a otros ámbitos directamente relacionados con los niños, tales como el tratamiento de datos para disposiciones testamentarias, de salud o de ideología, religión y creencia de los menores.

Así, en relación con la oferta directa de servicios de la sociedad de la información a menores, únicamente será lícito el tratamiento de los datos personales de menores de 16 años o, en caso de que el Derecho de un Estado miembro disponga una edad menor, pero en ningún caso inferior a los 13 años, si dicho consentimiento resulta dado o autorizado por el titular de la autoridad parental sobre el niño.

Si bien técnicamente aún existen dificultades para la verificación de la edad, el RGPD obliga al responsable del tratamiento a llevar a cabo esfuerzos razonables para verificar que el consentimiento ha sido dado o autorizado por el titular de la autoridad parental sobre el niño.

Estas normas directamente aplicables al ámbito de la privacidad no afectarán a las normas generales del Derecho contractual de los Estados miembros, como son las normas en materia de validez, formación o efectos de los contratos en relación con un niño, donde se aplica el principio de *lex specialis derogat generalis*[49].

[49] Cfr. Fellmeth, A. X., & Horwitz, M. (2009). *Guide to Latin in International Law*. Oxford University Press. Recuperado a partir de https://books.google.es/books?id=p5RsPgAACAAJ.

Asimismo, el Considerando 38 dedica una particular referencia a los menores, con el fin de asegurar la adecuada protección de su privacidad en relación con los riesgos a que actualmente quedan expuestos: *«Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos en relación con el tratamiento de datos personales. Esto se aplica particularmente a la utilización de datos personales de niños con fines de mercadotecnia o creación de perfiles de personalidad o de usuario y a la obtención de datos de niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la autoridad parental no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños».*

Otra novedad se encuentra en el *principio de transparencia* equiparado al derecho de información vigente que asiste a los ciudadanos. El Considerando 53 del Reglamento regula este principio en relación con el principio de calidad de los datos, según el cual el responsable de tratamiento queda obligado a obtener únicamente los datos necesarios para la finalidad para la que se recogen y en atención al estado de la tecnología en el momento de recabar los datos.

Según el tenor literal del Considerando 53, *«El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro y, además, cuando proceda, se visualice. Esta información podría facilitarse también en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente cuando, en determinadas situaciones, como la publicidad en línea, la proliferación de agentes y la complejidad tecnológica de la práctica, resulte difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, los datos personales que le conciernen. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y llano que puedan comprender con facilidad».*

En el ámbito del derecho al olvido, el Reglamento se detiene en considerar cómo se aplica respecto de los menores de edad, incluso cuando hayan dejado de serlo en relación con informaciones pretéritas. Se subraya en el Considerando 65 que *«Este derecho es pertinente, en particular, si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quisieran suprimir tales datos personales, especialmente en Internet. El interesado debe poder ejercer esta derecho no obstante el hecho de que ya no es un niño. Sin embargo, la posterior conservación de los datos debe ser lícita cuando sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el desempeño de un cometido en interés público o en el ejercicio de una autoridad oficial otorgada al responsable, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público o con fines de investigación científica e histórica o estadísticos o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.»*

3.9. Cumplimiento normativo.

El Reglamento General establece el nombramiento de un «responsable de la protección de datos» (*Data Protection Officer*, DPO) para ayudar a las autoridades competentes a garantizar el cumplimiento de la normativa sobre protección de datos.

Otro instrumento para garantizar el cumplimiento es la «evaluación de impacto en la privacidad» (*Privacy Impact Assessments*, PIA), aplicable en el caso de que sea probable que un tratamiento suponga un riesgo elevado para los derechos y las libertades de personas físicas. En tales supuestos, las autoridades competentes deberán efectuar previa o simultáneamente una evaluación del posible impacto de un tratamiento determinado, en particular cuando se utilice una tecnología nueva.

3.9.1. Delegado de Protección de Datos.

La figura del DPO ("*Data Protection Officer*") o Delegado de Protección de Datos ha sido objeto de intensos debates sobre su carácter obligatorio y universal para todas las entidades e instituciones. Finalmente el Delegado de Protección de Datos regulado en el Reglamento será un instrumento voluntario para el responsable y el encargado del tratamiento, aunque con excepciones, con el fin de velar por el cumplimiento legal y técnico en las entidades.

Conviene aclarar que el *Data Protection Officer* es una figura necesaria para las entidades, empresas, instituciones o cualquier agente que "maneje" datos personales y, si bien en la práctica sería la persona ocupada de las cuestiones sobre protección de datos y privacidad, su designación no exime a la propia institución u organización de responsabilidad de cuanto se haga con los datos de las personas ni del cumplimiento de las normas del Reglamento.

Existe así la obligación de contratar un Delegado de Protección de Datos (DPO) en organizaciones e instituciones públicas y en entidades con más de 250 trabajadores. En el caso de entidades con menos de 250 empleados, será obligatorio el DPO cuando necesiten un seguimiento sistemático y periódico de los datos personales tratados para la monitorización o investigación de mercados, análisis de riesgos o datos crediticios o de solvencia patrimonial, así como cuando traten los citados datos catalogados de especialmente protegidos.

Las entidades podrán determinar y ampliar las funciones y responsabilidades de los Delegados de Protección de Datos, que deberá tener al menos los siguientes cometidos:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales de las obligaciones que les incumben en virtud del Reglamento y otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el Reglamento, en otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización;

e) cooperar con la autoridad de control;

f) actuar como punto de contacto de la autoridad de control para las cuestiones relacionadas con el tratamiento de datos personales incluida la consulta previa, y consultar en su caso, sobre cualquier otro asunto.

El responsable y el encargado del tratamiento estarán obligados a designar un delegado de protección de datos para garantizar el cumplimiento de la normativa cuando una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función jurisdiccional, realicen el tratamiento, cuando las actividades principales consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados a gran escala; o cuando tales actividades consistan en el tratamiento a gran escala de las categorías especiales de datos (datos de origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, biométricos, de salud o vida y orientación sexuales y datos relativos a condenas penales y delitos).

Con la incorporación de DPO se pretende dar una mayor fuerza a la figura del Responsable de Seguridad, que es la persona que actualmente se debe asignar en las organizaciones para velar por el correcto cumplimiento de la normativa de protección de datos.

La diferencia más significativa entre el Responsable de Seguridad y el Delegado de Protección de Datos es la exclusividad de éste último en sus funciones. El DPO ya no será, como hasta ahora, la persona que se designaba como Responsable de Seguridad, ocurriendo que, sin apenas justificación, se elegía a profesionales sin la adecuada capacitación. El DPO será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar los cometidos contemplados en el Reglamento.

En este sentido, el DPO podrá pertenecer a la plantilla del responsable o del encargado del tratamiento o desempeñar las funciones de delegado en el marco de un contrato de servicios. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

El RGPD aclara que el responsable o el encargado velarán por que el DPO no reciba ninguna instrucción en lo que respecta al ejercicio de estos cometidos. No será destituido ni sancionado por el responsable o el encargado del tratamiento por desempeñar sus cometidos. El delegado de protección de datos informará directamente al más alto nivel de dirección del responsable o del encargado del tratamiento.

3.9.2. Evaluación de impacto en la privacidad.

El auge de nuevos modelos de negocio, comunicaciones y medios tecnológicos, tales como las tecnologías *wearables*, el auge del *Internet of Things* (IoT), la progresiva implantación de soluciones de cruzamiento masivo de datos o *Big Data*, el procesamiento de datos sensibles de carácter religioso o ideológico, el tratamiento de datos biométricos, la geolocalización, las nuevas fronteras en el ámbito de la ciberseguridad, hasta el *fingerprinting* o la tecnología de reconocimiento facial en redes sociales, dan lugar a nuevos riesgos que pueden tener consecuencias con carácter simultáneo en distintas localizaciones, lo que da valor al desarrollo de este marco unificado a nivel europeo.

El Reglamento General exige en su artículo 33 la evaluación de impacto relativa a la protección de datos cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas.

En estos casos, el responsable del tratamiento está obligado, antes del tratamiento, a realizar una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales. Una única evaluación servirá para abordar una serie de operaciones de tratamiento similares que planteen riesgos elevados similares.

En particular, el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si este ha sido nombrado, al llevar a cabo la evaluación de impacto relativa a la protección de datos.

La evaluación de impacto para la protección de los datos deberá llevarse a cabo en los siguientes casos:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y a partir de la cual se tomen decisiones que produzcan efectos jurídicos en relación con los particulares o que les afecten significativamente de algún otro modo;

b) tratamiento a gran escala de las categorías especiales de datos, o de los datos relativos a las condenas penales y delitos; y

c) observación sistemática de una zona de acceso público a gran escala.

La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados;

d) las medidas previstas para afrontar los riesgos, como las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a probar la conformidad con el Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

3.9.3. Sanciones.

Otro aspecto relevante a tener en cuenta es el de las sanciones. El nuevo Reglamento pretende unificar los criterios comunitarios para la imposición de sanciones, así como aumentar su cuantía para garantizar la mayor protección de un derecho fundamental como la privacidad.

Se amplía así el alcance de las sanciones contra los responsables y encargados del tratamiento que no cumplan con la normativa, y se faculta a las Autoridades Nacionales de Protección de Datos a imponer sanciones administrativas de hasta 20 millones de euros o el 4% de su volumen de negocios total anual.

Además, se reconoce el derecho de los interesados a presentar una reclamación a la Autoridad de Control nacional, así como su derecho a la tutela judicial efectiva ante los órganos jurisdiccionales de cualquier Estado Miembro.

3.9.4. Supervisión e indemnización

El Reglamento General refuerza la posición de las *Autoridades* como instancias independientes y especializadas de tutela del derecho a la protección de datos. Se amplían y armonizan sus poderes, sobre todo mediante el reconocimiento de una potestad sancionadora generalizada.

Además se establecen mecanismos de cooperación y coordinación entre las Autoridades de control, cuyo máximo exponente será la figura del nuevo Consejo Europeo de Protección de Datos, heredero, con nuevas funciones y capacidades, del actual Grupo de Trabajo del artículo 29.

No obstante estos significativos avances, la actividad de las Autoridades dependerá en gran medida de cómo se articule el funcionamiento del llamado mecanismo de ventanilla única. En su formulación original, el mecanismo suponía que una sola autoridad sería responsable de la supervisión de la actividad de responsables y encargados con varios establecimientos en la Unión. Esta opción, aplaudida por algunos y criticada por muchos, presentaba graves problemas en términos de protección eficaz de los derechos de los ciudadanos.

El resultado final, después de complejas negociaciones, parece positivo en tanto que recoge soluciones que permitirán una participación directa y efectiva de las autoridades de protección de datos en la defensa de los interesados de su estado miembro. Pero puede resultar excesivamente complejo y contiene algunos elementos de difícil aplicación práctica, en especial por la necesidad de coordinación de las autoridades concernidas.

4. Aplicaciones prácticas.

4.1. A quién y cómo afecta el nuevo Reglamento.

El nuevo Reglamento afecta a todas las entidades que recaben y procesen datos de carácter personal.

En la actualidad, dentro de la «sociedad de la información» es prácticamente universal que todas las entidades y organizaciones dispongan de una base de datos de contactos, miembros, clientes, empleados, etc.

Además, las entidades que traten datos sensibles (salud, origen racial, religión, vida sexual, etc.) están especialmente afectadas por las normas del Reglamento, por ejemplo por los especiales requisitos que conciernen a la información y al consentimiento de los interesados, que deberá ser claramente expreso y por tanto explícito, además de otras novedades como la obligatoriedad de designar un delegado de protección de datos (DPO).

Como novedad particular, el Reglamento es aplicable a entidades que, incluso sin estar establecidas en el territorio de la UE, dirigen sus bienes, servicios o actividades a usuarios europeos, con independencia de dónde se produzca el pago o se encuentre el establecimiento principal.

La relevancia de este Reglamento es total, sustituye a la Directiva 95/46/CE y es de aplicación directa en todos los Estados miembros. Es claro que la importancia para cualquier entidad es vital, porque a través de la regulación de la protección de datos se está protegiendo a los ciudadanos en general y a los afectados en particular.

4.2. Novedades particulares para las entidades.

Las novedades más relevantes para las entidades que procesan datos personales, sistemáticamente son las siguientes:

1) La aplicación del Reglamento es directa en todos los Estados miembros de UE, sin necesidad normativa de transposición a los ordenamientos internos de cada Estado miembro. Se trata de una única norma de protección de datos para todos los Estados de la UE.

2) Las medidas a adoptar e implementar tienen como base el riesgo que conlleve el tratamiento de los datos personales para el afectado.

   Será necesario designar un "Delegado de Protección de Datos" (DPO), realizar una "Evaluación de impacto de la protección de datos" (PIA) o incluso una consulta previa al tratamiento de los datos personales con la autoridad nacional de protección de datos, si existe un alto riesgo para la persona a la que se refieren los datos en ausencia de la adopción de medidas por el responsable, para mitigarlo.

3) Nuevos principios de la protección de datos: transparencia, responsabilidad, protección de datos desde el diseño y por defecto.

4) Dos nuevos derechos que las entidades deberán garantizar: derecho al olvido y a la portabilidad de datos.

5) Datos sensibles: salud, origen racial, de carácter sexual, ideología, religión, creencias, etc., y también otros nuevos como los datos genéticos y datos biométricos.

6) El consentimiento para el tratamiento de los datos personales con carácter general debe ser no sólo "expreso" sino "claramente inequívoco", y además "explícito" en el caso de datos sensibles (salud, origen racial, religión, vida sexual, etc.). El responsable tendrá que ser capaz de demostrar que obtuvo el consentimiento necesario del titular de los datos personales.

7) Se abren nuevas posibilidades de transferir internacionalmente datos personales a terceros países, fuera de la UE o del Espacio Económico Europeo (EEE) en atención, por ejemplo, a un sector de actividad, como por ejemplo el de Cloud Computing.

8) Medidas de pseudonimización y anonimización de los datos personales: la pseudonimización no escapa a las disposiciones del Reglamento, que seguirán siendo aplicables ya que es posible identificar a la persona a la que se refieren los datos personales; la anonimización, siempre que sea irreversible y no constituir datos personales, no está sujeta al Reglamento.

9) Reducción significativa de burocracia para las entidades: se establece un sistema de 'ventanilla única' tanto para las organizaciones como para los interesados, que tendrán como interlocutora a una sola autoridad de control.

4.3. "Delegado de Protección de Datos" (DPO).

La figura del DPO queda definida así para las entidades:

1) Tendrán que ser profesionales que puedan acreditar formación y conocimientos especializados en materia de protección de datos.

2) Sus funciones serán básicamente asegurar el cumplimiento normativo de la protección de datos, haciendo compatible el funcionamiento de la organización, la consecución de los objetivos lícitos y legítimos de su actividad y la garantía del derecho a la protección de datos y la seguridad de la información; además será el interlocutor necesario con la Autoridad de Control de la Protección de Datos.

3) Su implantación será obligatoria.

4) El DPO puede establecerse a través de contratación externa o mediante designación dentro de la plantilla de la organización.

5) Deben contar con un DPO:

    a. todas las organizaciones públicas, a excepción de los tribunales en ejercicio de la potestad jurisdiccional,

    b. entidades que desarrollen "profilling" (registro y análisis de las características psicológicas y de comportamiento de una persona, a fin de evaluar o predecir sus capacidades en un determinado ámbito o para ayudar en la identificación de las categorías de personas),

    c. entidades que requieran monitorización periódica y sistemática de los titulares de los datos a gran escala (desde solvencia patrimonial, investigación de mercados o en controles asociados a la productividad y hasta el análisis de riesgos),

    d. entidades cuya actividad principal consista en tratamiento de categorías especiales de datos (datos que revelen el origen racial o étnico, ideología, religión o creencias filosóficas, afiliación sindical, datos genéticos, y el tratamiento de datos biométricos para identificar unívocamente a una persona, así como los relativos a la salud y vida y orientación sexual, y datos relativos a condenas y antecedentes penales) y cuando lo disponga el Derecho de la Unión o el del Estado miembro.

4.4. Sanciones por no cumplir con los requisitos del nuevo Reglamento.

El incumplimiento puede conllevar multas de hasta 20 millones de euros o, en el caso de las entidades, hasta el 4% de la facturación total a nivel mundial del año financiero previo, siendo aplicable la suma que sea mayor.

Estas sanciones para muchas organizaciones representarían una dura brecha económica que se puede evitar tomando las medidas legales y técnicas oportunas, con el tiempo suficiente y con carácter preventivo.

4.5. Soluciones aplicables.

Las soluciones para cada entidad deben ser aplicadas a medida, en cada caso particular, no siendo recomendable adoptar meras "soluciones estandarizadas", pues el inicial bajo coste puede conducir a muy caras consecuencias.

En función del volumen de procesamiento de datos o de la sensibilidad de la información, cada entidad deberá contratar a proveedores con la debida acreditación y profesionalidad.

La implantación seria de protección de datos debe atender a la actividad que desarrolla la entidad y, dentro de ella, al concreto tratamiento de datos personales de clientes, empleados, miembros, proveedores, etc., necesario para atender a sus finalidades y necesidades concretas en respuesta a sus estrategias, actividades y gestión interna.

La recomendación es hacer una consultoría a la medida de las necesidades de cada entidad. En principio, no implica necesariamente un coste difícilmente asumible por la organización y puede ser una inversión que también redunde en la fidelización de los interesados y en la optimización de la organización y de la productividad. El comportamiento del ciudadano ha evolucionado y considera preocupante que sus datos puedan no estar seguros, de modo que es necesario considerarlo internamente como un requisito para la confianza del interesado, y es una inversión más que un coste.

5. Conclusiones.

La cercana aprobación definitiva del Reglamento General de Protección de Datos en Europa presenta expectativas positivas. La existencia de un marco legal sólido y uniforme de alcance europeo, adecuadamente actualizado a las necesidades del espacio tecnológica, permitirá no sólo liberar el potencial del Mercado Digital, el fomento de la innovación, la creación de empleo y la generación de riqueza, sino también salvaguardar el derecho fundamental a la protección de datos de los ciudadanos europeos o residentes en Europa.

La regulación en desarrollo para el futuro próximo comporta que entidades y organizaciones habrán de cumplir sus obligaciones en la adopción de medidas de protección adecuadas a los riesgos, la realización de evaluaciones de impacto, una mejor gestión de crisis e incidencias en ciberseguridad, así como de la implementación de mecanismos jurídicos y técnicos que garanticen la seguridad, confidencialidad e integridad de los datos personales y de toda aquella información asociada, también mediante el reconocimiento y atención de los dos nuevos derechos, el derecho al olvido digital y a la portabilidad de los datos personales.

El avance técnico debe correr parejo a la definición de nuevos mecanismos alternativos que redunden en el acceso y aseguramiento de la información, así como en la transparencia y en el respeto a los principios de protección de datos: limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, rendición de cuentas.

Las principales novedades del Reglamento General de Protección de Datos son:

1. Nuevos derechos de los ciudadanos: derecho al olvido y derecho a la portabilidad de los datos de un usuario de un sistema de tratamiento electrónico a otro.
2. La creación de la figura del Delegado de Protección de Datos (DPO, *Data Protection Officer*).
3. Obligación de realizar Análisis de Riesgos y Evaluaciones de Impacto para determinar el cumplimiento normativo.

4. La obligación de registrar documentalmente las operaciones de tratamiento, tanto por parte de los Responsables de Fichero como por los Encargados de Tratamiento.
5. Nuevas notificaciones a la Autoridad de Control: brechas de seguridad y autorización previa para determinados tipos de tratamiento.
6. Nuevas obligaciones de información al interesado, mediante un sistema de iconos armonizado para todos los países de la UE.
7. Incremento de la cuantía de las sanciones.
8. Aplicación del concepto "Ventanilla Única" (*One-stop-shop*), para que los ciudadanos interesados puedan efectuar trámites, aunque afecten a autoridades de otros estados miembros.
9. Establecimiento de obligaciones para nuevas categorías especiales de datos.
10. Nuevos principios en las obligaciones de información: transparencia y minimización de datos.

La nueva regulación presenta considerables ventajas:

a) Supondrá una armonización y unidad de criterio en la aplicación y garantía de los derechos de los ciudadanos europeos en materia de privacidad y protección de datos. Destaca el carácter pionero del continente europeo en garantizar y velar por estos derechos fundamentales.

b) Incorpora el derecho al olvido y el derecho a la portabilidad.

c) Ofrece un enfoque preventivo más que sancionador, con incidencia en la privacidad desde el diseño o privacidad por defecto, en las evaluaciones de impacto y códigos de conducta y en la necesidad del DPO *(Data Protection Officer)*.

d) Contiene una nueva regulación de los mecanismos de supervisión y control correspondientes a las autoridades nacionales.

e) Incluye un régimen sancionador completo, que detallan tanto las agravantes como las atenuantes.

f) En el ámbito particular de la geoinformación, define significativamente entre los «datos personales» toda información sobre una persona física identificada o identificable, incluido cualquier identificador y también los datos de localización. Asimismo, en relación a la «elaboración de perfiles», se incorpora toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física y, en el ámbito geoespacial, alude expresamente a la ubicación o movimientos de la persona física.

g) El futuro Consejo Europeo de Protección de Datos va a tener la capacidad de adoptar decisiones jurídicamente vinculantes y para el mecanismo de ventanilla única, relacionado también con el derecho al olvido.

h) Se reducirá la burocracia, pues ya no será obligatorio para las empresas inscribir sus ficheros en los registros de las autoridades nacionales.

Sumario.