Derechos y obligaciones de los ciudadanos/as en el entorno digital

Coordinador principal: Diego López Garrido
Autoras: Mª Mercedes Serrano Pérez
y Celia Fernández Aller

Documento de trabajo 195/2017

FUNDACIÓN alternativas

FUNDACIÓN alternativas

Derechos y obligaciones de los ciudadanos/as en el entorno digital

Coordinador principal: Diego López Garrido
Autoras: Mª Mercedes Serrano Pérez
y Celia Fernández Aller

Documento de trabajo 195/2017

Diego López Garrido

Es economista, catedrático en Derecho Constitucional y letrado de las Cortes. Preside el Consejo de Asuntos Europeos de la Fundación Alternativas. Ha sido secretario de Estado para la UE desde abril de 2008 hasta diciembre de 2011, y coordinó la presidencia española de la UE de 2010. Fue portavoz del Grupo Socialista en el Congreso (2006-2008) y diputado durante seis legislaturas. Perteneció a la convención que elaboró el Tratado Constitucional Europeo, antecedente del vigente Tratado de Lisboa, en representación de las Cortes Generales (2002-2003). Es autor del libro *La Crisis de las telecomunicaciones: el fenómeno desregulador en Estados Unidos y Europa* (FUNDESCO, Madrid, 1989).

Mª Mercedes Serrano Pérez

Doctora en Derecho, es profesora de Derecho Constitucional en la Universidad de Castilla-La Mancha. En la actualidad forma parte de la asociación Jurista de la Salud y del Grupo de Confidencialidad y Protección de Datos de la Sociedad Española de Epidemiología (SEE), habiendo realizado diferentes informes para dicha sociedad, entre ellos el Informe sobre la Propuesta de Reglamento Europeo de Protección de Datos y las Enmiendas presentadas (2013). Con una amplia actividad docente e investigadora, ha publicado diversos libros y artículos y participado en numerosos seminarios nacionales e internacionales.

Celia Fernández Aller

Doctora en Derecho, es profesora titular interina de la Universidad Politécnica de Madrid (UPM). Con docencia en grado y postgrado centrada en derechos fundamentales y nuevas tecnologías, es responsable de las cuestiones jurídicas del grupo de investigación Sistemas Telemáticos para la Sociedad del Conocimiento: telemedicina y discapacidad (UPM) y coordinadora de diversos proyectos de investigación sobre Enfoque Basado en Derechos Humanos. Colaboración en proyectos europeos relacionados con la ciberseguridad (CIPHER; CAMINO) y publicaciones de diversa índole.

Este estudio ha sido financiado por Telefónica.

ISBN: 978-84-15860-84-6
DL: M-5245-2018

Maquetación: Vera López López
Edición: Andrea Fernández Novo y Sergio Torres Pascual

Impreso en papel ecológico

Contenido

Prefacio

¿Hacia una constitución digital?

Hace casi 30 años, en 1989, FUNDESCO (Telefónica) inició la colección "Contextos de Telecomunicaciones". Tuve el honor de escribir la obra que inauguró dicha colección. Llevaba por título: *La Crisis de las Telecomunicaciones. El fenómeno desregulador en Estados Unidos, Japón y Europa*. Fue un libro producto de un viaje de varias semanas a Estados Unidos, en el que pude ver la transformación asombrosa que teníamos ante nosotros.

En el capítulo inicial del libro señalaba un cambio económico fundamental, que despuntaba a finales del siglo XX: "la información deviene un factor clave y determinante de la producción (…) de las sociedades industriales avanzadas". La causa era una mutación tecnológica capital: la revolución electrónica, es decir, el conjunto de técnicas que utilizan las variaciones de las magnitudes eléctricas para captar, tratar, transmitir y difundir una información.

Sobre este punto de partida –la electrónica- hay tres evoluciones tecnológicas que han servido de desencadenante (*trigger*) de lo que hoy llamamos "lo digital". Primero, las informaciones, de cualquier naturaleza, pueden ser hoy ya tratadas de manera similar: es la numerización (digitalización) de la información, que permite utilizar una imagen, cifras, textos escritos, sonidos, de manera perfectamente homogénea. Segundo, el almacenamiento de la información es cada vez más barato (baja de los costes de los circuitos integrados). Y, tercero, la transmisión de la información ha sufrido una transformación formidable: las centrales electrónicas pueden transmitir datos, sonidos e imágenes a velocidades vertiginosas.

De ahí que el sector de las telecomunicaciones se haya convertido en el más estratégico de todos los sectores productivos de la economía terciarizada en que vivimos en todo el mundo, ya no solo en Occidente.

Cuando escribí todo eso, hace casi tres décadas, no imaginaba la explosión de Internet, de las redes sociales, de los *smartphone*, ni la hegemonía aplastante de

las cinco más grandes corporaciones del mundo: Apple, Google, Microsoft, Amazon y Facebook, que tienen cuatro puntos en común: son transnacionales, son empresas tecnológicas, son norteamericanas y son las sociedades que más dinero ganan eludiendo el pago de impuestos merced a la ingeniería fiscal que son capaces de desarrollar, haciendo imposible la competencia de *startups* y de empresas más pequeñas a las que, si es necesario, absorben sin ningún problema. Y algo más: las empresas de Internet no pagan nada por utilizar esta Red en su negocio; quien paga es el usuario final. Esto también es producto del fenómeno de la digitalización de las comunicaciones y la producción de bienes tangibles e intangibles.

Es una dinámica imparable que ha cambiado nuestras vidas. En el siglo XXI se ha consolidado el reinado del dato después de vencer al viejo reinado de la transmisión de voz. El *big data* es la técnica imbatible de crecimiento, alimentada más y más por los satélites de comunicaciones, por las autopistas de la información, por las múltiples aplicaciones en la Red, por el comercio digital y, cómo no, por el propio consumidor de Internet al que entrega sus datos una y otra vez. Los datos se han convertido en el recurso más valioso del mundo, que The Economist equipara a lo que el petróleo significó en el siglo XX.

La galaxia digital es tan "invasora" que representa mejor que cualquier otra realidad lo que calificamos como globalización. De ahí que afecte a actividades y a derechos individuales y sociales tan importantes como la alimentación, la vivienda, la educación, la información, la libre expresión, la asociación, el trabajo, la intimidad, los espectáculos, la cultura, las relaciones familiares. Prácticamente cualquier hecho que forma parte de nuestra vida, directa o indirectamente, está –o estará- condicionado o atravesado por el mundo digital. Cualquier sistema de producción, cualquier tipo de trabajo está o estará digitalizado.

La realidad, se ha dicho siempre, va por delante del Derecho, de la Ley. La digitalización no es una excepción (en 2010, el iPhone tenía solo tres años de vida). De ahí que sea una exigencia urgente del momento la regulación de algo

tan difícilmente regulable como es Internet (véase el debate actual sobre la neutralidad en la Red), los mensajes por WhatsApp o Twitter, el tratamiento de millones de datos. Y todo presidido por "su majestad el algoritmo", que lo mismo pervierte y manipula una campaña electoral que contribuye a romper la burbuja de una crisis financiera. Un algoritmo es capaz de identificar tendencias dentro de los mismos datos, analizar hábitos sociales, hacer predicciones de conductas comerciales (o incluso criminales) en base al *big data*. Y eso por no hablar de la capacidad disruptiva que posee la inteligencia artificial, en la que están invirtiendo cantidades millonarias las corporaciones mayores del mundo.

La Unión Europea ha abordado la protección de la intimidad personal, del derecho a la personalidad y la dignidad humana mediante el Reglamento General de Protección de Datos, que entrará en vigor en mayo de 2018, completado en España por el Proyecto de Ley Orgánica de Protección de Datos. Es destacable la expansión territorial que realiza el Reglamento: afecta a entidades que no tienen su sede en la Unión Europea pero inciden en monitorizar la conducta de los ciudadanos a través de sus datos. Esto ya lo había puesto de relieve el Tribunal Europeo de Derechos Humanos en su sentencia Google versus Agencia Española de Protección de Datos (4 de mayo de 2016), lo que obliga a clarificar cuándo hay conflicto de leyes (entre UE, EEUU y China, por ejemplo) en esta materia.

Pero la digitalización es mucho más que la protección de datos. Por eso, queda mucho por hacer en el campo de los derechos y las obligaciones de los ciudadanos/as en el entorno digital.

Es enormemente compleja esta cuestión, con derechos que se contraponen (libertad de expresión versus derecho a la intimidad; derecho al anonimato en la Red frente a la protección ante injurias o insultos en la Red; vigilancia sobre mensajes delictivos frente a la libertad de circulación de datos en la Red, etc.). Es tan amplio el impacto de la revolución digital que cambia la propia doctrina jurisprudencial a la hora de interpretar el alcance legal de una investigación sobre un delito. Al Tribunal Supremo de EEUU se le ha planteado si la 4ª

enmienda de la Constitución norteamericana –que prohíbe investigaciones no razonables (*unreasonable searches*)- es de aplicación a la indagación de la policía sobre un enorme número de datos de una persona sospechosa, datos personales que solo tienen en su poder las compañías operadoras de Internet (caso Carpenter versus EEUU, nº 16-402, que para algunos defensores de la Constitución puede convertirse en el más importante caso sobre privacidad electrónica en el siglo XXI).

Nuestro Tribunal Supremo (Sala de lo Penal) acaba de dictar recientemente (10 de marzo de 2016) una sentencia en la que aplica la modificación del artículo 588 de la Ley de Enjuiciamiento Criminal (por Ley Orgánica 13/2015) en la que requiere autorización judicial expresa para la investigación sobre dispositivos electrónicos incautados fuera del domicilio del investigado.

Es ingente el cúmulo de desafíos regulatorios ante nosotros sobre el inabarcable y siempre sorprendentemente innovador mundo de lo digital. En la resolución final de la última reunión del G-20 en Hamburgo, el 6-7 de julio de 2017, se afirma que un objetivo común de esta formación política de las mayores potencias mundiales es enfrentarse a los retos de lo que llama "mundo interconectado".

Se ha llegado a hablar de la necesidad de una "Constitución Digital". Quizá nos parezca exagerado este término, aunque vaya entrecomillado, pero lo cierto es que lo digital tiene tales dimensiones –y está tan poco tratado por el derecho con una perspectiva coherente y estructurada– que no sería descabellado afrontar el estudio –y la posterior decisión política– del universo digital desde los numerosos ángulos jurídicos que posee.

Por el momento, el derecho de lo digital, los derechos ciudadanos afectados y los de las personas jurídicas, empresas, que trabajan en ese campo, merecería ser objeto de un texto o textos recopiladores o refundidores de la "selva legal" en que se encuentra el a veces anárquico entorno digital. Estoy hablando de una "Constitución Digital" –materialmente hablando, no formalmente– que

introdujera seguridad jurídica en este complejo territorio. Para empezar, ahora que se habla en España de reforma constitucional; si la hubiera, habría que modernizar la insuficiente y defensiva alusión que esta hace a que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (art. 18.4). En muchas de las demás constituciones europeas no hay ni siquiera mención al tema.

La Unión Europea, en el contexto de su estrategia Agenda Digital para Europa, debería trabajar por una Directiva que desarrolle la Carta de Derechos Fundamentales de la Unión Europea, que solo se refiere a dicha cuestión digital en términos parecidos a la Constitución Española, proclamando que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. (...) Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación" (arts. 8.1 y 2 de la Carta).

Ni la Constitución de 1978 ni la Carta europea de Derechos Fundamentales garantizan un derecho decisivo para afrontar la revolución digital: el derecho al acceso a Internet. Hoy existe lo que se define como "brecha digital" dentro de un país y entre países. Sin la garantía del acceso a Internet es inútil hablar de "igualdad real y efectiva" de los ciudadanos, como dice el artículo 9 de la Constitución española, que cumplirá el 6 de diciembre de 2018 cuarenta años.
De esa "Constitución Digital" –española, europea e internacional- en el horizonte debiera formar parte un código ético o "Declaración de Derechos y Obligaciones Digitales" para regular el comportamiento de todos los sujetos –privados, públicos, empresariales- que protagonizan la dinámica de lo que hemos llamado entorno digital. De todo ello vamos a hablar en el presente trabajo.

Diego López Garrido
Coordinador principal

1. Introducción

La sociedad digital ha supuesto una transformación radical en todos los ámbitos de nuestras sociedades y ha obligado a reconfigurar los derechos y las obligaciones de la ciudadanía. Tanto los poderes públicos como las empresas y otras instituciones se ven afectados también por los cambios que se producen a ritmo vertiginoso.

Este documento se detiene en los impactos que la digitalización de la sociedad produce en los derechos más fundamentales de las personas. Comienza con las repercusiones en el principio de igualdad referidas a la situación de la accesibilidad electrónica, o acceso de las personas con diversidad funcional a las nuevas tecnologías. Sin duda la normativa está avanzando, aunque queda camino por recorrer, de forma que cualquier actor, público o privado, se vea obligado a ciertas pautas de accesibilidad.

Además, se aborda sintéticamente el concepto de brecha digital y su impacto en los derechos de las personas; también el acceso electrónico de los ciudadanos a los servicios públicos en el marco de lo que se ha denominado la administración electrónica. Se alude, así mismo, a la neutralidad en la Red, que impide la utilización abusiva de esta por algunos operadores y proveedores de Internet para favorecer sus intereses comerciales, condicionando la capacidad de acceder a los datos que circulan por Internet.

Se analizan los impactos de los cambios tecnológicos en el derecho a la educación, en la libertad de expresión y de información, en el derecho de asociación y participación. Un detenimiento especial han merecido el derecho a la identidad online y a la protección del anonimato, como derechos que surgen de la utilización intensiva de Internet y del tratamiento digital de volúmenes inabarcables de información personal.

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. En este momento contamos con un Reglamento Europeo de Protección de Datos que será aplicable en España desde mayo de 2018, que ha obligado a adaptar nuestra norma interna sobre protección de datos. Estos cambios han supuesto una reconsideración grande del derecho fundamental a la protección de datos, adaptándolo a las implicaciones de las tecnologías emergentes en la autodeterminación informativa de los individuos.

En el REPD se describen los nuevos derechos que la configuran, como el derecho al olvido o la portabilidad de los datos; se reconocen nuevos actores, como el delegado de protección de datos; se prioriza un enfoque más proactivo de responsabilidad exigible al responsable del tratamiento; se obliga a notificar las brechas de seguridad; se consagran los principios de privacidad por defecto y privacidad en el diseño; aparece la necesidad de los estudios de impacto en la privacidad.

Además de los derechos, el documento recuerda la importancia de las obligaciones, tanto de particulares como de Estados y de actores privados. Todos ellos están llamados a respetar los derechos de la ciudadanía, a reforzar la confianza digital –en la que descansan muchos de los avances de nuestra sociedad digitalizada-, a promover la interoperabilidad de aplicaciones de Internet y servicios de comunicación y mensajería para mejorar la experiencia del usuario y favorecer la competencia. Todos deben contribuir a una mayor transparencia de las condiciones de uso de los servicios de Internet, a transformar los modelos educativos y los procesos de enseñanza mediante la adopción de tecnologías digitales y servicios basados en recursos y estándares abiertos. En definitiva, todos están llamados a contribuir a una mayor gobernanza de Internet.

Junto a los retos jurídicos, se resalta la importancia de los retos éticos, que aparecen como elemento esencial para superar los desafíos que supone la

sociedad de la información y el conocimiento. Se señala la importancia de un análisis de los aspectos éticos y sociales con anterioridad al despliegue de las nuevas tecnologías, siguiendo los marcos teóricos que existen para ello. Esto es una interpelación clave dirigida al sector de la industria tecnológica. Por otro lado, se recoge el papel de los códigos de conducta, muestra de la autorregulación, y el papel de las certificaciones y los sellos de privacidad, que permitirán aumentar la confianza y la transparencia.

El documento también se detiene en los retos en el ámbito de la ciberseguridad y en el papel de las estrategias europea y española relativas a este tema. Termina con un capítulo de propuestas que sintetizan las líneas de acción surgidas de un análisis profundo de los impactos de la transformación digital en los derechos de las personas. Con ello pretende contribuirse al diseño de políticas públicas y corporativas que sirvan en mayor medida a situar a la persona en el centro de los avances de la sociedad digital.

2. El impacto de la sociedad digital en los derechos de los ciudadanos en España y ámbito europeo

2.1. Introducción

La sociedad digital ha transformado nuestro modo de vida en todos los aspectos imaginables. Los avances en la tecnología nos han abierto hacia una nueva etapa cuyos inicios podemos datar con más o menos precisión, pero los continuos avances en la materia mantienen todavía abierto el periodo señalado. En efecto, los cambios en la tecnología marcan un ritmo trepidante que impiden, en parte, determinar con exactitud el sentido concreto del término "sociedad digital". Quizá por ello, lo único que podemos mantener como acuerdo de mínimos en relación con la expresión y con su propio significado hace alusión a "la transformación profunda de los modos de vida tradicionales, programas de ajuste económico, cambios industriales, alteraciones en las formas de gobierno de educación y de trabajo e, incluso, aunque se hable poco de ello, transformaciones muy profundas de personalidad y del modo de ser de los individuos" (Pérez Tornero, 2005: 248). Por una parte, los cambios afectan a los medios y a los instrumentos en los que se proyecta y desenvuelve la vida de los ciudadanos y, por otra parte, los cambios que ha provocado la sociedad digital afectan a la propia condición humana desde una perspectiva individual, es decir, influyen en la construcción de la personalidad del individuo, en sus relaciones con el entorno y con el resto de personas.

El sujeto "agresor" frente al ejercicio de los derechos fundamentales también ha experimentado una transformación en el mundo tecnológico. La sociedad digital ha ampliado el espectro de situaciones en que puede provocarse una lesión en los derechos de los individuos y la extensión de escenarios posibles amenazadores para los derechos fundamentales.

Junto a la eventual amenaza que representa el mundo digital, no podemos ignorar las **innumerables ventajas** que para el ser humano aporta la tecnología aplicada

racionalmente. La utilización sensata de los medios tecnológicos ha de llevarnos, más que nunca, a valorar y reflexionar sobre las **obligaciones** que han de respetar tanto los sujetos que disponen del control de los medios de la sociedad de la información como de los sujetos que acceden a ellos, que se han convertido en productores de contenidos y que interactúan en la Red. En la sociedad digital se habla más que en ningún otro momento de códigos de conducta, pautas de actuación, etc., de obligaciones que en un caso adquieren naturaleza jurídica, y por tanto son exigibles judicialmente, y en otros no, adoptando la forma de medidas, recomendaciones, directrices, etc., cuya finalidad es reglamentar la actividad en la Red.

Por lo que respecta al poder público, el paradigma del Estado social en el mundo digital reconvierte al Estado en un motor de impulso, de cambio, de lucha por la igualdad real, que ha de contemplar las posibilidades tecnológicas como un instrumento útil para los individuos y la sociedad, sin que su uso pueda generar desigualdad. Por tanto, las prestaciones sociales que el Estado ha de proveer para alcanzar la igualdad real han de contemplar la implantación de la tecnología como parte de las mismas, y de una manera universal y generalizada. En este sentido, se habla de "brecha digital" para aludir a la ruptura que supondría para la sociedad el acceso de una parte de la misma a los beneficios tecnológicos y la negación a la otra parte, que quedaría limitada en el ejercicio democrático de sus derechos. Serían estos últimos, "los nuevos pobres" de la sociedad digital, los ciudadanos carentes de medios y recursos tecnológicos; carencia que limitaría sus aspiraciones y sus capacidades para convertirse en ciudadanos plenos y con igualdad de oportunidades.

En el campo público, la sociedad digital también abre las posibilidades del *e-government* a través de una administración electrónica que, con altas dosis de transparencia y accesibilidad, aspira a facilitar los trámites con el ciudadano: permisos, licencias, presentación de documentos, pagos; una relación administración-ciudadano que puede también despersonalizar dicha relación. Por otro lado, se potencia desde la Red la participación democrática de los ciudadanos, una mayor implicación en los procesos de toma de decisiones; participación online que conlleva

también otros riesgos, como la eficacia real de dicha participación o la operatividad de la democracia electrónica.

En este marco de la sociedad digital, el Derecho ha comenzado a elaborar una regulación que facilite la convivencia armónica entre las posibilidades de la tecnología y los derechos de los ciudadanos y que extienda y regule la sociedad digital a todos. En Europa, esa intervención normativa se plantea desde la aprobación de la **Agenda Digital para Europa** en el año 2010, que, en el marco de la normativa comunitaria y de la integración europea, pretende "impulsar la economía europea aprovechando las ventajas económicas y sociales sostenibles del mercado único digital"[1]. La visión europea añade, a las posibilidades digitales y los derechos de los ciudadanos, el aspecto económico, que constituye un parámetro esencial de actuación europea. La Agenda Digital para Europa está concebida como una de las siete iniciativas de la **Estrategia Europa 2020**. Para la UE, en el marco de dicha Agenda, los aspectos fundamentales que hay que abordar guardan relación con tres elementos esenciales: **el mercado único digital, el acceso de las personas con discapacidad y la relación del ciudadano con los servicios públicos**. El mercado digital aporta la perspectiva económica de las potencialidades digitales. Desde este punto de vista, las posibilidades de crecimiento económico a través del comercio electrónico son una nueva fuente de expansión que, a su vez, requiere de otros factores, potenciados también desde la UE, como el empleo sostenible y el desarrollo y adaptación de derechos y obligaciones laborales en el entorno digital. En segundo lugar, el acceso a las tecnologías de las personas con discapacidad, o lo que es igual, la inclusión digital, que exigirá de los poderes públicos un esfuerzo económico y de infraestructuras con el fin de no originar y mantener la brecha digital y proveer a los ciudadanos de las condiciones necesarias para no sufrir una discriminación que podría afectar a múltiples aspectos de su vida. En tercer lugar, los servicios públicos en un sentido amplio, que abarque la relación entre ellos y los ciudadanos, lo que incluiría el modo de interactuar con estos últimos en sectores como la sanidad, la educación, etc.

[1] Agenda Digital Europea, https://europa.eu/european-union/file/1501/download_es?token=3l7D0Fil, p. 3, visitada el 7-8-2017

Varias precisiones hay que tener en cuenta al abordar el estudio jurídico de la sociedad digital. La primera cuestión a resolver es si la regulación del ciberespacio requiere medidas jurídicas específicas o basta con una adaptación del marco jurídico propio de la sociedad analógica. Sin ser soluciones incompatibles y excluyentes, parece claro que la tendencia es la elaboración y adopción de normas específicas que regulen la realidad de la sociedad digital, solución que facilita el conocimiento y aplicación de normas complejas; aunque también encontramos referencias específicas a aspectos de la sociedad digital en normas tradicionales, dirigidas a regular materias que, de forma transversal, se ven afectadas por las tecnologías. En este sentido, y como característica del bagaje normativo del que hablamos, las normas relativas a la sociedad digital se suceden de modo vertiginoso en el tiempo, en consonancia con los avances tecnológicos. Así, en un periodo relativamente breve de tiempo se producen normas que derogan la regulación anterior, relativamente reciente, lo que obliga a un esfuerzo interpretativo y a una adaptación constante a los cambios de los agentes implicados.

La segunda cuestión se refiere a la imposibilidad de regular este espacio común con criterios nacionales, modo en el que se han ido regulando otros espacios en los que la soberanía de los estados ha determinado el contenido de las normas a adoptar sobre los sectores a regular. En la sociedad digital no existen barreras tangibles o elementos diferenciadores que justifiquen una legislación diferente para cada Estado, al amparo de fronteras y realidades territoriales distintas, por lo que es preciso regular de modo global los aspectos digitales o, al menos, contemplar un conjunto de elementos comunes a todos los países, unos mínimos legislativos. En realidad, la diversidad legislativa es cada vez menor en el mundo globalizado en el que se desenvuelven las relaciones de todo tipo y, así, las regulaciones jurídicas se ajustan a parámetros acordados por gran parte de la comunidad internacional, especialmente en aquellos países que forman parte de una integración supraestatal, como es el caso de la UE. Aquí, la armonización legislativa es una premisa jurídica esencial, lograda por medio de la adopción de Directivas, que han de ser traspuestas al ordenamiento interno, o de Reglamentos, normas de aplicación directa.

Para una mejor comprensión de las afectaciones que la sociedad digital introduce en el campo de los derechos, analizaremos los derechos fundamentales cuyo ejercicio y protección se ven transformados **en y por el mundo digital**. Un estudio de este tipo debe partir de la concepción de la igualdad como principio esencial de un Estado social y democrático de Derecho y su manifestación en el mundo digital.

2.2. El principio de igualdad: la accesibilidad web

La igualdad, como concepto relacional y como ausencia de discriminación, se manifiesta en el mundo digital en la **facilidad para acceder a la Red**, es decir, en la puesta a disposición de los ciudadanos de instrumentos que posibilitan desenvolverse en la sociedad digital actual a un nivel equivalente de recursos y de prestaciones que, negadas, provocarían una quiebra del principio de igualdad material. Esta idea se identifica con el concepto de "**accesibilidad web**"**.**

La garantía del acceso igualitario de todos los ciudadanos a las posibilidades de la Red corresponde al poder público que, en el Estado social, ha de remover todos los obstáculos para conseguir la igualdad real (art. 9 CE) y promoverla, con acciones dirigidas a facilitar prestaciones digitales a la población, para evitar la denominada "brecha digital". Esta brecha provocaría una desigualdad por motivos tecnológicos o de otra índole que podría afectar al ejercicio de diferentes derechos fundamentales de los ciudadanos (como el derecho a la educación, a la información, al trabajo, etc.) en condiciones de igualdad.

Es de obligada mención la sentencia del TEDH de Estrasburgo, de 18 de diciembre de 2012 (caso Ahmet Yildirim). En ella, el Tribunal admite que ninguna restricción a una fuente de información es compatible con el Convenio Europeo de Derechos Humanos. Y una fuente privilegiada de información es ya Internet, por lo que la restricción de acceso es una forma de violar la libertad de expresión e información. A este respecto, el TEDH cita reiteradamente la sentencia del Consejo Consultivo francés de 10 de junio de 2009. Otros países han introducido en el siglo XXI el acceso a Internet como un derecho básico: Estonia, Grecia, Finlandia, Alemania, Turquía, la OSCE. También en España en 2011 (García Mexía, 2017). El Consejo de Derechos Humanos de Naciones Unidas ha declarado en julio de 2016 el acceso a

Internet como un derecho humano, defendiendo, en su resolución, la "promoción, protección y disfrute de los derechos humanos en Internet". La resolución de UN anima a todos los países a facilitar el acceso a Internet a todos sus ciudadanos como un medio más para proteger la libertad de expresión. Asimismo, se insiste en la necesidad de reforzar la libertad y la seguridad en la Red y promover la educación tecnológica, en especial de mujeres y niñas. La resolución no es vinculante, pero su valor reside en el reconocimiento de las posibilidades de desarrollo y de progreso humano que supone Internet.

La **accesibilidad web** tiene como finalidad permitir que las páginas web puedan ser utilizadas por el mayor número de personas, con independencia de sus conocimientos tecnológicos o capacidades personales y al margen del equipo técnico empleado para el acceso a la Web. La accesibilidad web tiene dos perspectivas. En primer lugar, la accesibilidad **desde el punto de vista técnico** puede entenderse como un conjunto de principios jurídicos, éticos y de reglas técnicas que deben respetarse para diseñar, construir, mantener y actualizar los sitios web para ser más accesibles a los usuarios, definición de accesibilidad contenida en el considerando 2 de la Directiva UE 2016/2102 del Parlamento y del Consejo, de 26 de octubre de 2016, relativa a la accesibilidad de los sitios web y aplicaciones de dispositivos móviles de los organismos del sector público[2]. Aunque definida la accesibilidad en el contexto de la Directiva, nada impide que la idea que subyace pueda ser extrapolable a un concepto más general de accesibilidad que hace referencia a las reglas técnicas que facilitan a los usuarios el acceso a Internet. Un concepto que incluye no solo el acceso a la web desde el punto de vista técnico sino también **desde la perspectiva de contenidos,** en segundo lugar**,** lo podemos encontrar en la siguiente definición: la "accesibilidad web es la posibilidad de que cualquier persona, independientemente de sus capacidades personales y de las características técnicas del equipamiento utilizado, tenga acceso a toda la información y funcionalidades de un sitio web"[3]. Por tanto, el acceso a la Red en condiciones de igualdad ha de garantizar tanto la inexistencia de limitaciones tecnológicas (a servicios) como la inexistencia de restricciones de contenidos (informativos, de relación). "Se dice que una página o sitio Web es accesible cuando

[2] DOUE L327, de 2.12.2016.

[3] Definición disponible en https://dialnet.unirioja.es/info/accesibilidad

está diseñado y construido para que sus contenidos y servicios estén disponibles para cualquier persona, con independencia de sus capacidades visuales, auditivas, cognitivas o motrices e independientemente de la tecnología que utilizan. Esto incluye: sitios y aplicaciones Web; navegadores Web y reproductores de medios; herramientas de creación de la Web y tecnologías Web en desarrollo."[4] Las recomendaciones para alcanzar y mantener la accesibilidad han sido recogidas por la Web Accessibility Initiative (WAI), que ha desarrollado directrices y pautas consideradas estándares internacionales con el objetivo de facilitar la introducción del concepto de accesibilidad web.

El **acceso igualitario a Internet** reconoce el derecho a todos los ciudadanos a acceder en condiciones de igualdad, con la eliminación de obstáculos económicos, sociales, tecnológicos y de cualquier tipo que puedan provocar una brecha digital. Especial atención en cuanto a favorecer la accesibilidad merecen determinados colectivos, que pueden ver mermado su acceso a Internet, como son los discapacitados, las personas mayores, las mujeres, la población rural. Los primeros, hay que recordar, son objeto de dedicación particular en la Agenda Digital para Europa. De "**inclusión digital**" habla el texto europeo para referirse al reto de acercar Internet a las personas desfavorecidas.

2.2.1. La accesibilidad web de personas discapacitadas

En el mundo hay 650 millones de personas con discapacidad. El colectivo de la discapacidad incluye a las personas que se encuentran en una situación de desventaja social -como consecuencia de una deficiencia física, mental, intelectual o sensorial a largo plazo-, que al interactuar con diversas barreras puede impedir su participación plena y efectiva en la sociedad en igualdad de condiciones con el resto de individuos, es decir, sin que su limitación pueda suponer un obstáculo para su dignidad y desarrollo pleno.

Los poderes públicos han de velar para que la igualdad material sea un hecho para estos colectivos. La **accesibilidad universal** está definida en el artículo 2.k del Real

[4] Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas por la que se aprueba la Guía de comunicación digital para la Administración General del Estado, BOE, núm. 79, de 2 de abril de 2013, p. 9 y ss., disponible en http://www.administracionelectronica.gob.es)

Decreto-Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, como "la condición que deben cumplir los entornos, procesos, bienes, productos y servicios, así como los objetos, instrumentos, herramientas y dispositivos, para ser comprensibles, utilizables y practicables por todas las personas en condiciones de seguridad y comodidad y de la forma más autónoma y natural posible. Presupone la estrategia de «diseño universal o diseño para todas las personas», y se entiende sin perjuicio de los ajustes razonables que deban adoptarse"; definición semejante a la contenida en la Ley 51/2003, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, que la definía como "la condición que deben cumplir los entornos, procesos, bienes, productos y servicios, así como los objetos o instrumentos, herramientas y dispositivos, para ser comprensibles, utilizables y practicables por todas las personas en condiciones de seguridad y comodidad y de la forma más autónoma y natural posible" (norma derogada por el RD 1/2013, de 29 de noviembre).

En relación con el acceso a las tecnologías, la situación de dificultad se manifiesta especialmente en una sociedad cada vez más tecnológica y puede provocar un aislamiento de la persona. La tecnología puede levantar una barrera intangible que impida accesos a la educación, a la sanidad, al trabajo, etc., de las personas discapacitadas. Desde el **Foro Europeo de la Discapacidad** (EDF)[5] en su **Manifiesto sobre la Sociedad de la Información y la Discapacidad** (1999) se señala que: "Las personas con discapacidad no tienen garantía de que la Sociedad de la Información vaya a mantener la promesa de convertirse en una sociedad totalmente accesible para todos. Si la tecnología no se adapta a las necesidades y las capacidades individuales o no se normaliza según las necesidades de accesibilidad de las personas con discapacidad y de otros consumidores, si la información mayoritaria del futuro se procesa de forma que algunos grupos de usuarios con discapacidad queden excluidos, la Sociedad de la Información constituirá una amenaza para las personas con discapacidad".

[5] Disponible en http://www.edf-feph.org/

Se trata en definitiva de no crear barreras o eliminar las que puedan existir, ya que en la sociedad tradicional las barreras eran físicas y visibles, pero las barreras en las comunicaciones son obstáculos o dificultades en la comprensión, lectura y captación de mensajes verbales, visuales y en el uso de los medios técnicos disponibles para las personas con distinta clase y grado de discapacidad. La tecnología no puede avanzar sin eliminar este tipo de barreras.

A nivel internacional, la **Convención de las Naciones Unidas sobre el derecho de las personas con discapacidad,** de 13 de diciembre de 2006, ratificada el 30 de marzo de 2007, cita la accesibilidad como principio de la Convención (art. 3.f), y señala como obligación general "promover la disponibilidad y el uso de las nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones", así como dar información sobre las mismas (art. 4.h). El principio general a la accesibilidad, que incluye la identificación y eliminación de obstáculos y barreras de acceso, se aplicará a "los servicios de información, comunicaciones y de otro tipo, incluidos los servicios electrónicos y de emergencia" (art. 9). Así pues, resulta una obligación de los Estados el "promover el acceso a las personas con discapacidad a los nuevos sistemas y tecnologías de la información y las comunicaciones, incluida Internet" (art. 9). Pero la Convención insta también a los **entes privados** a proporcionar información y servicios en formatos que las personas con discapacidad puedan utilizar y tener acceso, incluso, dice el artículo 21, a través de Internet. Esta llamada de atención a los entes privados es una consecuencia de la transformación operada en la sociedad digital, como decíamos al comienzo de nuestro trabajo, en la que el sector privado ha ocupado un espacio importante de las relaciones sociales, por lo que debe exigirse a los entes privados un nivel de compromiso elevado, a través de códigos éticos y de conductas para ajustar su actuación en el campo tecnológico a principios y reglas que sean compatibles con el interés general. Ello con independencia del sometimiento de los mismos a la legalidad y a los principios y derechos constitucionales.

Por lo que respecta a la legislación española, la primera referencia a la accesibilidad, y a un plazo y reglas para lograrla se encuentra en la disposición adicional quinta de la Ley 34/2002, de 11 de julio, de sociedad de la información y comercio

electrónico[6] (LSSICE), según la cual, "Las Administraciones públicas adoptarán las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005". Respecto de la norma se pueden hacer dos precisiones. En primer lugar, la referencia a los "criterios de accesibilidad al contenido generalmente reconocidos", que es la expresión de la norma para aludir al nivel de accesibilidad exigible a las administraciones públicas, resulta indeterminada e imprecisa, y por ello es difícil de observar y cumplir. Las últimas normas sobre accesibilidad y discapacidad han intentado corregir esta ambigüedad. En segundo lugar, hay que determinar qué son las administraciones públicas. Según el artículo 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[7] (LRJSP), tienen la consideración de administraciones públicas, "La Administración General del Estado, la Administración de las Comunidades Autónomas, las Entidades que integran la Administración local, así como los organismos públicos y las entidades de derecho público previstos en la letra a) del apartado 2". El apartado 2 de la citada norma se refiere a los organismos públicos y entidades de derecho público vinculados o dependientes de la Administración Pública[8].

La Disposición Adicional quinta LSSICE establece que, a partir del 31 de diciembre de 2008, las páginas web de las administraciones públicas satisfarán como mínimo el nivel medio de los criterios de accesibilidad al contenido generalmente reconocido. La **obligación incumbe tanto a las páginas web cuyo diseño o mantenimiento esté financiado con dinero público como a las páginas web de empresas o entidades que se encargan de gestionar los servicios públicos**. En particular, dice la norma esta obligación recae en los **Centros Educativos, de formación y universitarios, así como los centros que reciban financiación pública.** Además, las páginas web de las administraciones públicas deben facilitar un contacto para poder transmitir las dificultades de acceso al contenido de las páginas de Internet y la

[6] BOE núm. 166, de 12 de julio de 2002.

[7] BOE núm. 236, de 2 de octubre de 2015.

[8] En el caso de la Administración General del Estado, según el art. 84.1 a) LRJSP son organismos públicos vinculados o dependientes de la Administración general del Estado: Organismos autónomos y Entidades Públicas Empresariales.

posibilidad de trasladar cualquier queja, sugerencia o consulta. Por último, quedan también obligadas por la norma a adaptar sus páginas web y hacerlas accesibles, "las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información", disponiendo para ello de la fecha tope del año 2008, así como "las páginas de Internet que sirvan de soporte o canal a las redes sociales en línea, desarrolladas por entidades cuyo volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.101.121,04 euros", teniendo que satisfacer dichos criterios a partir del 31 de diciembre de 2012. En ambos casos se trata del nivel medio de accesibilidad al contenido generalmente reconocido. Habrá que determinar cuál es el nivel medio de accesibilidad. Por otro lado, los plazos han sido modificados por la legislación posterior.

Como aclaración, es preciso tener en cuenta que la accesibilidad a contenidos digitales en el ámbito de la Administración Pública para personas con discapacidad es una particularidad de la obligación general de accesibilidad que tienen respecto de todos los ciudadanos y que recoge la Directiva 2016/2102, y a la que deberán adaptarse las normas españolas antes del 23 de septiembre de 2018, 21 meses después de la entrada en vigor de la Directiva citada.

El Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, vuelve a establecer en la disposición transitoria única un conjunto de plazos para la adaptación de las páginas de Internet de las administraciones públicas diferente, según se trate de páginas nuevas o de páginas ya existentes. El Real Decreto menciona la necesidad de ajustarse, tanto las páginas nuevas como las existentes, a la prioridad 1 de la Norma UNE 139803:2004, dentro de los plazos señalados y ambas a la prioridad 2 de la misma Norma UNE a partir del 31 de diciembre de 2008. La Norma UNE 139803:2004, actualizada por la Norma UNE 139803:2012, es una norma española que recoge los requisitos de accesibilidad para los contenidos web y se basa en las

pautas y directrices recogidas en la Iniciativa de Accesibilidad a la Web (Web Accesibility Initiative) del Consorcio Mundial de la Web (World Wide Web Consortium)[9]. La Norma UNE concreta y precisa los criterios de accesibilidad que se han de cumplir solventando la indeterminación de la LSSICE. La Norma UNE abarca la mayoría de los tipos de discapacidad: visual, auditiva, física, del habla, cognitivas, del lenguaje, de aprendizaje y neurológicas y también las personas de edad avanzada, como un colectivo más que precisa una atención especial para facilitar el acceso a las TIC. La Norma UNE contiene **tres niveles de accesibilidad**, siguiendo los niveles establecidos en la Iniciativa de Accesibilidad a la Web, niveles A, AA o doble A y AAA o triple A (que ya estaban recogidos en la Norma UNE 139803:2004). La Norma UNE del 2012 se diferencia de la 2004 en que la vigente está basada en los criterios contenidos en la WCAG 2.0[10] y las prioridades que recogía la norma del 2004, que clasificaban los requisitos, ahora, en la Norma del 2012 las prioridades se identifican con niveles, es decir, nivel A, nivel AA y nivel AAA.

Para cumplir los requisitos de cada nivel se han de observar una serie de criterios que varían según el nivel correspondiente. En lo que a las **administraciones públicas** se refiere, y por aplicación del Real Decreto 1494/2007, los portales web de dichas administraciones deben ser accesibles a **nivel doble AA** (antigua prioridad 2)[11], lo que significa que los portales han de cumplir una serie de obligaciones. Las obligaciones se agrupan en cuatro principios[12]:

- Principio 1: **perceptible**. La perceptibilidad hace referencia al modo en el que la información y los componentes de la interfaz se presenten al usuario para que pueda percibirlos. La exigencia de percepción de los contenidos implica que se deben prever alternativas a la información facilitada, a través del

[9] Otras normas a tener en cuenta en relación con la accesibilidad son: la Norma CWA 1554:2006, norma que recoge la base de la certificación europea en accesibilidad web, y la *Guía de Comunicación Digital para la Administración General del Estado* (Ministerio de Hacienda y Administraciones Públicas, 2012: 6 y ss.)

[10] Web Content Accesibility Guidelines (WCAG 2.0), que constituye una recomendación internacional sobre cómo hacer más accesibles los contenidos digitales a las personas con discapacidad, disponible en http://www.w3.org/TR/WCAG20/

[11] El W3C (World Wide Web Consortium), consorcio que elabora recomendaciones y estándares para consolidar el crecimiento de la World Wide Web, exime a los autores de la páginas web que no cumplan los requisitos señalados siempre y cuando parte del contenido esté fuera de su control y opten por la Declaración de Conformidad Parcial (http://www.w3.org/TR/2008/REC - WCAG20 - 20081211/#conformance-partial).

[12] Ministerio de Hacienda y Administraciones Públicas (2012: 9 y ss.)

formato que precise el usuario, o bien a través de textos, o voz, o braille, o formato visual claro. La adecuación del contenido a los diferentes formatos no puede ir en detrimento de la pérdida de información o de la estructura. En resumen, es requisito obligatorio para la satisfacción del cumplimento de la perceptibilidad presentar alternativas textuales para los contenidos que no son textos y los contenidos no textuales deben tener igualmente una alternativa textual, excepto determinadas situaciones ya previstas, como son controles, entrada de datos, contenido multimedia, tiempo dependiente, pruebas, CAPTCHAS, contenidos dirigidos a crear experiencias sensoriales.

- Principio 2: **operable**. Los componentes de la interfaz de usuario y navegación han de ser operables, o lo que es lo mismo, las funcionalidades puedan ser manejadas desde el teclado, con tiempo suficiente y razonable para leer y usar el contenido deseado, encontrar el contenido de manera fácilmente intuitiva, medios que ayuden a navegar, y saber dónde se encuentra el usuario en su proceso de navegación, para lo cual los títulos, etiquetas y encabezados deben hacer alusión explícita al tema concreto, incluir más de un camino para acceder a una página concreta dentro del sitio web, facilitar un proceso que evite los bloques de contenidos que se repiten en varias de las páginas de las administraciones públicas, etc.
- Principio 3: **comprensible**. Principio que hace alusión directa tanto al manejo como a la información de la interfaz y a su fácil comprensión. La comprensión de los contenidos textuales va ligada a su legibilidad. Entre los requisitos obligatorios propios de este principio podemos citar la indicación del idioma al desarrollar un sitio web, mantener el mismo orden de repetición en los mecanismos de navegación a disposición del usuario, si la página web presenta campos para introducir datos por parte del usuario se deben incorporar etiquetas aclaratorias, mecanismos para detectar los errores cuando se introducen datos, facilidad para que el usuario lo pueda identificar. Si la operación implica compromisos legales o transacciones financieras, debemos asegurar que el envío de la información es reversible y que se ofrece al usuario la posibilidad de revisar, confirmar o corregir los posibles errores antes de que la operación sea definitiva.

- Principio 4: **robusto.** Según este principio, "El contenido debe ser suficientemente robusto como para ser interpretado de forma fiable por una amplia variedad de aplicaciones de usuario, incluyendo las ayudas técnicas"[13]. Se trata de "maximizar la compatibilidad con las aplicaciones del usuario, ya sean actuales o futuras, y las ayudas técnicas"[14].

Estos criterios deberían estar presentes en la elaboración de las páginas web de las administraciones públicas. Las medidas perceptibles, operables, comprensibles y robustas se recogen también en el artículo 1 de la Directiva 2016/2102, para los dispositivos móviles.

Dentro de la legislación española hay que hacer referencia también al Real Decreto-Legislativo 1/2013, de 29 de noviembre por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad, que, además de contener la definición de accesibilidad universal que ya hemos señalado más arriba, indica que las medidas específicas para garantizar la igualdad de oportunidades, la no discriminación y la accesibilidad universal se aplicarán, además de a los derechos regulados en el Título I de esta norma, al ámbito de las telecomunicaciones y sociedad de la información (art. 5.a). El artículo 24 de la citada norma señala que:

> "Las condiciones básicas de accesibilidad y no discriminación para el acceso y utilización de las tecnologías, productos y servicios relacionados con la sociedad de la información y de cualquier medio de comunicación social serán exigibles en los plazos y términos establecidos reglamentariamente.
> No obstante, las condiciones previstas en el párrafo anterior serán exigibles para todas estas tecnologías, productos y servicios, de acuerdo con las condiciones y plazos máximos previstos en la disposición adicional tercera.
> 2. En el plazo de dos años desde la entrada en vigor de esta ley, el Gobierno deberá realizar los estudios integrales sobre la accesibilidad a dichos bienes o servicios que se consideren más relevantes desde el punto de vista de la no discriminación y accesibilidad universal".

La Disposición adicional tercera aludida establece los plazos siguientes para que el acceso y utilización de las tecnologías, productos y servicios relacionados con la

[13] Ministerio de Hacienda y Administraciones Públicas (2012:13).

[14] Ministerio de Hacienda y Administraciones Públicas (2012:14).

sociedad de la información y de cualquier medio de comunicación social se adecúen a la ley según esta distinción:

- Productos y servicios nuevos, incluidas las campañas institucionales que se difundan en soporte audiovisual: 4 de diciembre de 2009.
- Productos y servicios existentes el 4 de diciembre de 2009, que sean susceptibles de ajustes razonables: 4 de diciembre de 2013.

Por otra parte, las administraciones públicas promoverán medidas de fomento y defensa de la igualdad de oportunidades y en ese marco podrán adoptar todas las acciones necesarias para que se supriman las disposiciones normativas y prácticas contrarias a la igualdad de oportunidades, así como establecer las medidas para evitar cualquier forma de discriminación por motivos de discapacidad (art. 69 y ss.).

La Directiva 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre, de accesibilidad de los sitios web y aplicaciones para los dispositivos móviles de los organismos del sector público, que habrá de implementarse en el ordenamiento interno de los Estados miembros en el plazo de 21 meses desde su entrada en vigor, vendrá a mejorar la accesibilidad a los sitios web del sector público, y mejorará y previsiblemente sustituirá las medidas contenidas en el RD 1494/2007, es decir, el cumplimento del nivel AA de garantías según la WCAG 2.0 (prioridad 1 y 2 de la Norma UNE). La Directiva pretende homogeneizar los requisitos de accesibilidad de los sitios web del sector público, estableciendo bases comunes que rompan la fragmentación del mercado interior. Es decir, de nuevo el objetivo del mercado digital único en el seno de la Unión. De ese modo se reduciría la incertidumbre para los desarrolladores, señala la Directiva en su considerando 9, y se fomentaría la interoperabilidad. La homogeneización de las medidas nacionales redundaría en un beneficio económico y social para los organismos y empresas del sector público de la Unión que, al ampliar su oferta de servicios en línea o servicios móviles, podrían captar más clientes y beneficiar a un mayor número de ciudadanos. Por supuesto la Directiva se enmarca en las medidas de accesibilidad para discapacitados, en el marco de las diferentes normas europeas e internacionales sobre la materia.

Como **aspectos destacados en la Directiva** 2016/2102 que habrán de ser tenidos en cuenta en su incorporación a la normativa nacional señalamos:

- La Directiva se aplica a las aplicaciones móviles desarrolladas por las administraciones públicas, lo que implica un paso más en la regulación de los mecanismos de la sociedad digital. En este caso, y dependiendo de la finalidad para la que se ha creado la aplicación, dicho mecanismo significa, sin duda, un nuevo medio de comunicación con el ciudadano. Por ejemplo, existen aplicaciones que ofrecen la posibilidad al ciudadano de comunicar a la Administración incidencias callejeras, e incluso mandar una foto de la incidencia, por ejemplo un árbol caído, o el destrozo de mobiliario urbano, etc. En el campo de la sanidad, las aplicaciones móviles permiten cada vez realizar más trámites con el ciudadano, así como recibir una información precisa sobre servicios sanitarios. Las aplicaciones móviles pueden habilitar un tipo de comunicación de notificaciones mucho más rápido y eficaz con el ciudadano. Hay que tener en cuenta que las aplicaciones móviles no deben contener toda la información de la Administración Pública, sino la información necesaria para cumplir el objetivo de la *app*. Incluir más información de la estrictamente necesaria podría quebrar el principio de accesibilidad en su principio comprensible. Por otro lado, para que las aplicaciones móviles de las administraciones públicas cumplan su cometido de mejorar la vida de los ciudadanos deben tener la publicidad necesaria para que todo ciudadano las conozca y deben poder adaptarse a cualquier pantalla y dispositivo móvil desde el punto de vista técnico, esto es, debe procurarse un mantenimiento adecuado, de manera que su uso no se convierta en un inconveniente para el ciudadano, más que en una ventaja.
- Cada Estado miembro debe establecer un organismo supervisor del cumplimento de las obligaciones que se contienen en la Directiva y en la normativa de desarrollo (art. 9).
- Se establece también un mecanismo de seguimiento de dicho cumplimiento (art. 8.2).
- Mejorará las condiciones de la accesibilidad de los portales web de las páginas de la administraciones públicas.

- Actualización periódica de una declaración de accesibilidad detallada, exhaustiva y clara de los sitios web por parte de las administraciones públicas y de las aplicaciones móviles (art. 7.1) y elaboración periódica de informes que permitan comprobar la conformidad de los sitios web y de las aplicaciones para dispositivos móviles del sector público, con los requisitos de accesibilidad de perceptible, operable, comprensible y robusto (art. 8.1).

En resumen, será necesario esperar para comprobar la adaptación de la Directiva al ordenamiento español y su cumplimiento. La Directiva fija como plazo para el cumplimento de todos los criterios señalados el año 2022.

2.2.2. El acceso electrónico de los ciudadanos a los servicios públicos

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos ha sido derogada por la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[15] (LPACAP). Sin embargo, la Ley que recoge y actualiza los principios sentados por la norma derogada es la LRJSP, que, en su artículo 3.2, alude a los medios electrónicos como el medio de relación entre las administraciones públicas y con sus organismos públicos y entidades vinculadas o dependientes, de forma que se asegure "la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados". Asimismo, el artículo 38 realiza una definición de la sede electrónica como la dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones, bajo la titularidad de la Administración Pública u organismos públicos en el ejercicio de sus competencias (art. 38 LRJSP). La Administración es responsable de la integridad veracidad y actualización de la información y los servicios que resta dicha sede electrónica. Los principios a los que ha de sujetarse la creación de dichas sedes electrónicas son los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. Debe garantizarse la identificación del órgano titular de la sede, así como los mecanismos para formular sugerencias y quejas. La norma alude también a

[15] BOE núm. 236, de 2 de octubre, de 2015.

la necesidad de establecer sistemas que permitan la seguridad en las comunicaciones. El apartado quinto del artículo 38 de la LRJSP recoge la referencia a la accesibilidad de las informaciones, servicios, y transacciones, de acuerdo con las normas establecidas al respecto, estándares abiertos y los que sean de uso generalizado de los ciudadanos. El artículo 39 de la LRJSP alude al portal de Internet como el punto de acceso bajo la titularidad de la Administración Pública que permite el acceso a través de Internet de la información publicada y de la sede electrónica. En lo que respecta a la concreción de los principio parecía más detallada la Ley 11/2007 derogada, pues, en la vigente, los principios, además de carecer de definición, parecen diluirse en la redacción de la referencia a la sede electrónica. En realidad el portal de Internet de una administración pública es un sitio web que contiene enlaces a otras páginas web, por lo que le son de aplicación todos los criterios y normas ya relatados en el apartado anterior que parecen pasar desapercibidos en la LRJSP. Quizá hubiera sido deseable una referencia más clara y expresa a los criterios de accesibilidad, dado que lo que parece imponerse en el futuro es la Administración electrónica. En cualquier caso, la formación mediante cursos, seminarios, guías, prácticas y demás elementos habrá de ser una constante en la actuación de la Administración.

La LPACAD recoge las peculiaridades de las relaciones de los ciudadanos con la Administración a través de trámites electrónicos en sus artículos 12 y 43. El artículo 12 de la LPACAD recoge la obligación de las administraciones públicas de garantizar la relación de los interesados con la Administración a través de medios electrónicos, y facilitando su utilización. Queda a la elección de la personas física el medio para relacionarse con la Administración Pública, para el ejercicio de sus derechos y obligaciones, salvo para los que sea obligatorio la utilización de medios electrónicos (art. 14 LPACAD), es decir, que se trate de personas jurídicas; entidades sin personalidad jurídica; quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para relación con la Administración Pública en el ejercicio de su profesión, incluidos notarios y registradores de la propiedad; quienes representen a un interesado que está obligado a relacionarse electrónicamente con la Administración y los empleados de las administraciones públicas para los trámites y actuaciones que realicen con ellas en razón de su condición de empleado público. Reglamentariamente, las Administraciones podrán ampliar la obligación de

relacionarse mediante trámites electrónicos, tanto a determinados colectivos como a determinados procedimientos, siempre que quede acreditado que, por razón de su "capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos", cláusula que contiene una indeterminación y generalización en exceso amplia y por ello difícil de verificar con certeza. En este sentido será necesaria una formación electrónica que prepare para la utilización correcta de dichos instrumentos por medio de cursos, jornadas o guías que permitan a los diferentes colectivos citados el manejo solvente de los mismos, y por supuesto, la accesibilidad de la página web. Junto a ello, el artículo 43 de la LPACAD recoge las peculiaridades de las notificaciones a través de medios electrónicos que habrá igualmente que conocer para darse por notificado, o para entender que la solicitud realizada por quien corresponda ha sido rechazada.

Por otra parte, la LRJSP, establece en los artículos 38 y siguientes las reglas para el funcionamiento de la Administración Electrónica.

2.2.3. La brecha digital

La OCDE[16] definía la brecha digital como la "diferencia entre individuos, hogares, empresas y zonas geográficas a distintos niveles socio-económicos en relación a sus oportunidades **para acceder** a las TIC **y para usar** Internet para una extensa variedad de actividades".

La brecha digital va más allá del acceso, del "tener o no tener", y se considera la importancia del uso que se hace de las TIC, en particular de Internet. Los beneficios de la tecnología en el bienestar y el desarrollo social no se producen de forma directa y automática con la mera incorporación de la infraestructura.

Más aún, tampoco el mero uso de Internet es determinante. No es tan trascendente cuánta gente utiliza Internet, sino por qué y para qué lo utiliza. En este marco, los usos que se hacen son fundamentales para un concepto más complejo de la brecha digital y para valorar el impacto de las TIC en el desarrollo humano.

[16] Organización para la Cooperación y el Desarrollo Económico.

En el contexto actual de la sociedad red, la brecha digital está íntimamente ligada a otras brechas de desarrollo. Se trata de una relación recíproca en la cual las desigualdades se retroalimentan y **la imposibilidad de uso a las tecnologías** en las mismas condiciones para todas las personas, **se convierte en motivo de exclusión social** y económica. Castells mantiene que la rapidez del cambio tecnológico, junto con la debilitación de la estructura de la familia tradicional y la crisis del estado del bienestar, pueden llevar a un incremento de la fragmentación social y la consecuente exclusión de aquellos grupos sociales más desfavorecidos, al no disponer de la cualificación necesaria para hacer frente a dichas transformaciones.

Pero esta relación también se dar en sentido positivo, una mayor inclusión social promueve una mayor inclusión digital y a su vez un mayor desarrollo digital, como hemos visto en la sección anterior, puede ser motor de un mayor bienestar y desarrollo social.

Otra conclusión relevante sería el hecho de que, dado que no todos los usuarios de Internet tienen la misma capacidad para explotar los recursos que ofrecen las tecnologías de la información y la comunicación, esta desigualdad digital se traslada a la esfera política: aquellos que son más hábiles en Internet son más capaces de realizar actividades políticas en la Red y fuera de ella. Las diferencias no se han reducido en el tiempo, pero las habilidades digitales han aumentado de forma general, dando mayor acceso a recursos digitales políticos y no políticos a los grupos tradicionalmente menos favorecidos (Cantijoch, 2014).

Marco regulatorio e institucional

La existencia de políticas gubernamentales decididas en apoyo de la extensión de las nuevas tecnologías es un factor esencial. Estas políticas deben de integrarse en las estrategias de desarrollo. Pueden consistir tanto en inversiones directas como en la creación de un marco legal y regulatorio que promueva el acceso, uso y aprovechamiento de las TIC.

Los conceptos de Acceso y Servicio Universal (ASU) suelen orientar estas políticas. El **servicio universal** (SU) remite a la prestación del servicio en favor de los

particulares y los hogares. La Unión Europea, lo define como "el conjunto definido de servicios cuya prestación se garantiza **para todos los usuarios finales** con independencia de su localización geográfica, con una calidad determinada y un precio asequible". Garantizar el servicio de telefonía suele ser el primer paso, junto con el de radiodifusión y televisión; actualmente, muchos países incluyen el servicio de banda ancha. La Ley de Economía Sostenible aprobada en España en 2011 incorpora el acceso a Internet a una velocidad en sentido descendente de 1 Mb/s y extiende el derecho de acceso de los usuarios con discapacidad en condiciones equivalentes.

Por acceso universal (AU) se entiende, en cambio, un nivel públicamente compartido de servicio, entre otras cosas, mediante teléfonos de pago públicos o telecentros con Internet. Este objetivo es más adecuado y viable para países con bajos ingresos, y en muchos casos se proponen objetivos de SU de telefonía en zonas urbanas y de AU para telefonía en zonas rurales o acceso a Internet.

La zona de desnivel real de acceso es la que precisa de decisiones políticas proactivas para el logro del ASU, que pueden ser vía subvenciones, uso de fondos internacionales de acceso y servicio universal[17], reglamentaciones que utilicen los beneficios de las zonas más rentables en el apoyo de las zonas sin acceso, etc.

Pero además del acceso, también son fundamentales las políticas de fomento del sector TIC (Corea, China, Costa Rica o España, con el Plan Avanza) de forma que se pongan las bases para la apropiación y adaptación de las tecnologías al contexto local, y haga posible la innovación. Esto nos lleva a otro de los factores esenciales para el desarrollo digital.

[17] Los "fondos de acceso universal" son un mecanismo financiero establecido para crear un nivel adicional de incentivos económicos a la inversión privada en la expansión y provisión de redes, manteniendo las condiciones de mercado. Los fondos de acceso universal caben dentro de la definición del concepto del Banco Mundial de *Output Based Aid* (ayuda basada en resultados): "uso de subsidios explícitos, basados en los resultados, para complementar o sustituir los cargos al usuario, involucrando la contratación de prestación de servicios básicos (como infraestructura, salud, educación) a terceros, (como empresas privadas, ONGs, organizaciones comunitarias y eventual-mente un proveedor de servicios público)".

La medición de a brecha digital

Para poder hablar de brecha es necesario tener instrumentos para medir las diferencias. La Unión Internacional de Telecomunicaciones (ITU), organismo especializado de las Naciones Unidas para las TIC, utiliza desde hace años el **Índice de Desarrollo de las TIC (IDI)** en sus estudios para la Medición de la Sociedad de la Información, y para analizar la evolución de la brecha digital.

Este indicador recoge datos sobre algunos de los factores analizados anteriormente para obtener un valor que refleje el desarrollo digital de un país y predecir el impacto que las TIC tienen en el desarrollo social y económico del mismo. En concreto, valora la capacidad de dicho país para aprovechar las TIC en su desarrollo (*readiness*) en función de **la infraestructura y el acceso** a la misma; las **capacidades** de la población para hacer un buen uso de dichas tecnologías (midiendo principalmente los niveles de educación media y superior), y el **uso efectivo** que se hace de ellas[18].

Según el informe *La Sociedad de la información en España* (Fundación Telefónica, 2010), en nuestro país hay diferencias significativas en el uso de Internet en función de la edad (90% de los jóvenes entre 16 y 24 años, frente al 10% de las personas entre 65 y 74 años) y los ingresos (86% de personas de altos ingresos frente al 11% de personas con bajos ingresos), y no tanto en cuanto a la zona geográfica (64% en ciudades de más de 100000 habitantes frente al 47% en poblaciones de menos de 10000 habitantes) y género (5,7 puntos de diferencia a favor del uso de Internet por parte de los varones).

Durante el año 2016, se advierte que los internautas mayores empiezan a hacer un uso intensivo de Internet, lo que lleva a que la realización de actividades relacionadas con la productividad aumente en 6,7 puntos porcentuales y las relacionadas con el ocio en 16,7. De hecho, el ocio se destaca como la principal motivación para conectarse a Internet entre ellos, con un crecimiento de 13,1 puntos porcentuales hasta el 59,3% entre los internautas. Mientras, la comunicación con familiares y

[18] Hay otros indicadores como el NRI (Networked Readiness Index), "más complejo, que además de indicadores de infraestructuras, acceso, capacidades y uso, incorpora otros acerca del marco regulatorio o los impactos sociales y económicos del uso de las TIC" (World Economic Forum and INSEAD, 2012).

amigos baja en 13,6 puntos porcentuales y solo el 20,4% de ellos la considera su principal motivación para conectarse a Internet, casi igual que la motivación profesional o de productividad, mencionada por el 18,4%.

2.2.4.. La neutralidad en la Red

El respeto al principio de igualdad de oportunidades en la sociedad digital no puede concebirse sin el derecho a elegir libremente entre una variada oferta de dispositivos, aplicaciones, contenidos, etc., mercado que corresponde a los proveedores de servicios de Internet (en adelante PSI). El ejercicio del derecho de igualdad requiere el presupuesto primero de ausencia de limitaciones para escoger, lo que obliga directamente al operador de telecomunicaciones a no interferir ni en los servicios que ofrece ni en los contenidos.

La carencia de interferencias voluntarias se conoce como la neutralidad en la Red. La neutralidad en la Red exige no solo la ausencia de discriminación por cualquier motivo a la hora de acceder a contenidos digitales, sino también neutralidad respecto de los servicios a ofertar. La idea de neutralidad en la Red se conecta con una Internet abierta, "sujeta a estándares abiertos y a la libertad de conexión de Internet" (Ruiz Gómez). El mercado único digital a que aspira la Agenda Digital 2020 no podría concebirse sin el respeto a la neutralidad en la Red, pues, la falta de neutralidad implica que determinados contenidos o datos se han sustraído a la posibilidad de acceso por parte del usuario, lo que vulnera el principio de igualdad en su versión de accesibilidad a la Red y puede limitar también el derecho a la libertad de expresión.

La experiencia del consumidor no se ve afectada si un mensaje electrónico le llega pocos segundos después de haber sido enviado, pero una demora análoga en una comunicación vocal supondría una degradación significativa de la misma, o incluso la privaría por completo de sentido. Buena parte del debate sobre la neutralidad de la Red se centrará en la gestión del tráfico y en las condiciones en que resulta razonable[19].

[19] Comunicación de la Comisión al Parlamento Europeo al Consejo, al Comité Económico y social Europeo y al Comité de las Regiones: "La internet abierta y la neutralidad de la Red en Europa", 2011, p. 8.

García Mexía (2017) recuerda la reacción de la comisaria Meelie Kroes, en un discurso pronunciado en 2013, ante la utilización fraudulenta de la Red por algunos operadores y proveedores de Internet europeos para favorecer sus intereses comerciales, condicionando la capacidad de acceder a Internet de los ciudadanos. Kroes anunció la propuesta de la Comisión para regular la neutralidad en la Red basada en cuatro principios: competencia (entre operadores y servicios), innovación, transparencia (en favor de los consumidores) y libre elección de operadores.

La regulación actual sobre la neutralidad en la Red se contiene en el Reglamento (UE) 2015/2120, de 25 de noviembre, del Parlamento Europeo y del Consejo, por el que se establecen medidas en relación con el acceso a una Internet abierta (TSM)[20]. El Reglamento entró en vigor el 30 de abril de 2016 y como se sabe es una norma de aplicación directa, por lo que constituye la normativa vigente en materia de Internet abierta.

Las medidas recogidas en el Reglamento respetan el principio de neutralidad tecnológica, es decir, "no imponen el uso de ningún tipo particular de tecnología ni discriminan a su favor" (considerando 2).

El **objeto del Reglamento** (art. 1) es establecer normas comunes para salvaguardar un tratamiento equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a Internet y los derechos relacionados de los usuarios finales. El artículo 3 reconoce el **derecho de los usuarios** finales "a acceder a la información y contenidos, así como a distribuirlos, usar y suministrar aplicaciones y servicios y utilizar los equipos terminales de su elección, con independencia de la ubicación del usuario final o del proveedor o de la ubicación, origen o destino de la información, contenido, aplicación o servicio, a través de su servicio de acceso a Internet". Al mismo tiempo se reconoce la **obligación para los proveedores de servicios de acceso a Internet** de tratar "todo el tráfico de manera equitativa cuando presten

[20] Reglamento 2015/2120, de 25 de noviembre de 2015, del Parlamento Europeo y del Consejo, por el que se establecen medidas en relación con el acceso a un internet abierto y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) número 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión, DOUE L 310, de 26 de noviembre de 2015.

servicios de acceso a Internet, sin discriminación, restricción o interferencia, e independientemente del emisor y el receptor, el contenido al que se accede o que se distribuye, las aplicaciones o servicios utilizados o prestados, o el equipo terminal empleado". El artículo 4 incorpora las medidas de transparencia que garantizan el acceso a una Internet abierta.

El Reglamento europeo habla de la **Autoridad Nacional de Reglamentación,** en cada Estado miembro**,** para atribuirles la competencia de supervisión del cumplimiento de los principios 3 y 4 del Reglamento. Según el artículo 5, dicha Autoridad elaborará Informes anuales en relación con la función de supervisión realizada y los elevará a la Comisión y al ORECE (Organismo de Reguladores Europeos de Comunicaciones Electrónicas)[21]. Pues bien, la protección del usuario de redes es una obligación que corresponde, según el artículo 69.f de la Ley 6/2014 General de Telecomunicaciones, al Ministerio de Energía, Turismo y Agenda Digital, que, de acuerdo con su estructura orgánica, atribuirá dicha competencia al órgano correspondiente que es la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital[22]. Y el órgano que resuelve los conflictos entre los usuarios y operadores es la Oficina de Atención al Usuario de Telecomunicaciones.

El Informe elaborado por el órgano supervisor durante el año 2016 no ha detectado problemas significativos relacionados con el principio de neutralidad en la Red. Solo, dice el Informe, el 0,91% de las reclamaciones recibidas pueden relacionarse con dicho problema. Sin embargo, creemos que existe una ignorancia de la población acerca del verdadero significado de la neutralidad en la Red, que hace que las reclamaciones no sean numerosas.

En lo que se refiere a las sanciones, se tipifican las siguientes infracciones (en los artículos 77 y 78 de la Ley General de Telecomunicaciones):

- Artículo 77.17: Negativa a cumplir las condiciones de prestación de los servicios y explotación de redes de comunicaciones electrónicas.

[21] https://europa.eu/european-union/about-eu/agencies/berec_es

[22] *Informe sobre supervisión en España de normativa europea en materia de acceso a una Internet abierta*, Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, Ministerio de Energía, Turismo y Agenda Digital, 2016, p. 6.

- Artículo 78.8: Explotación de redes o prestación de servicios sin cumplir los requisitos exigibles.
- Artículo 77.37: Vulneración grave de los derechos de los usuarios finales.
- Artículo 78.11: Vulneración (no grave) de los derechos de los usuarios finales.

Por lo tanto, el incumplimiento de las obligaciones del Reglamento sería sancionado conforme a alguno de esos preceptos. Las sanciones podrían ascender a un máximo de:

- Infracciones graves (art. 77): 2 millones de euros.
- Infracciones leves (art. 78): 50.000 euros.

El acceso y el uso de la Red sin discriminación de ningún tipo solamente puede realizarse desde una perspectiva de gobernanza de Internet, con el sentido de globalización que incorpora el término gobernanza. La gobernanza debe evitar los abusos de fuerzas económicas que podrían con su poder imponer restricciones y limitaciones al uso de la tecnología, no solamente a partir de la discriminación de contenidos digitales sino del establecimiento de determinados requisitos que impidieran el acceso a la Red. La gobernanza debe impulsarse desde iniciativas internacionales, con el fin de no provocar paraísos digitales que permitieran a los sujetos dominantes escapar del respeto a las normas y del control por parte de los tribunales y pudieran de este modo originar un abuso y una lesión de los derechos de los ciudadanos.

En este nuevo contexto, las políticas privadas sobre contenidos de las plataformas globales deberían alcanzar un equilibrio entre lo legal y lo que se considera moralmente aceptable. Esto no es tarea fácil debido a la gran variedad de culturas existentes en el mundo, que se traducen en distintos valores y sensibilidades. Por ello, muchas empresas, a fin de aumentar su transparencia, han publicado manifiestos en los que se explican a los usuarios qué clase de contenidos pueden publicar y cuáles no.

Aun así, las plataformas digitales dominantes, apoyándose en las condiciones de uso de los servicios por ellos definidas, han bloqueado contenidos por razones puramente comerciales. Estos hechos han provocado una creciente preocupación en los mercados ante el desarrollo de prácticas supuestamente anticompetitivas. Sistemas operativos abiertos ofrecerían a los usuarios una mejor experiencia digital.

Desde el punto de vista del consumidor, **la interoperabilidad y la interconexión de los servicios son conceptos clave de la experiencia digital**. En la actualidad, muchos consumidores no concebirían que en los primeros momentos de la telefonía los usuarios de una compañía telefónica no pudieran llamar a los de otra. La interconexión entre distintos teléfonos a lo largo y ancho del planeta se ha podido establecer gracias al consenso sobre el uso de estándares internacionales.

Y a pesar de esta conquista en el campo de la comunicación tradicional, todavía hoy, muchos de los proveedores de servicios de Internet ofrecen servicios que no se interconectan entre sí, es decir, que no son interoperables o que no se basan en estándares abiertos. Este tipo de comportamientos podría limitar la competencia, la innovación o coartar la libertad de elección de los consumidores.

En estos asuntos, no debemos entender la neutralidad de la Red exclusivamente en lo relativo a los ordenadores, también se refiere a la conexión a través de *smartphones* o cualquier otro dispositivo.

Otro asunto relacionado con la neutralidad de la Red es el de la **información abierta**. La información es uno de los pilares clave de la economía digital. Los usuarios, las empresas y la sociedad esperan que los servicios sean cada vez más personalizados y se basen en sus necesidades. La idea de tener "libre acceso" a determinados datos está ganando apoyos entre los gobiernos, las administraciones públicas y todas las actividades con financiación pública, como la investigación científica. A finales de 2011, 28 países ya disponían de plataformas con datos públicos. La mayoría de ellas están relacionadas con campos importantes para la sociedad como la salud, la meteorología y el medioambiente, la delincuencia, la educación o el tráfico.

Los datos abiertos ofrecen un impresionante abanico de posibilidades para las administraciones, las empresas y los ciudadanos. Tan solo en los 27 Estados de la UE se calcula que el impacto económico directo de los datos abiertos en la economía fue de 32.000 millones de euros aproximadamente en 2010, con un índice de crecimiento anual del 7%. Los beneficios potenciales abarcan desde la mayor eficacia para las organizaciones tanto del sector público como privado, a un mayor crecimiento económico y del empleo.

También supone una mejora sustancial en la transparencia de los organismos públicos y una mayor accesibilidad y potencial participación de los ciudadanos en asuntos públicos. La disponibilidad de los datos abiertos podría ayudar a resolver muchos de los problemas económicos y sociales actuales, ya que reduciría el consumo de energía y los niveles de contaminación, optimizaría el tráfico y mejoraría la asistencia sanitaria. Este es el motivo por el cual las administraciones públicas están actuando activamente, tanto a escala regional como nacional. Por ejemplo, las instituciones europeas están animando a los Estados miembros a que pongan a disposición de la ciudadanía el mayor volumen de información pública posible. La UE también está desarrollando un marco jurídico común para la reutilización de este tipo de información[23].

En EEUU el tema va por otros derroteros. En estos días (diciembre de 2017), la FCC ha cambiado la consideración de las operadoras de telefonía, que han pasado de ser servicios de telecomunicación sujetos a las normas de esta agencia, a servicios de información, que se rigen únicamente por la libre competencia.

Este cambio afecta a tres aspectos relevantes: el bloqueo de contenidos, dejando que las empresas prohíban aplicaciones que no acepten sus condiciones; la ralentización de servicios para priorizar aquellos por los que se pague una cantidad adicional y la posibilidad de priorizar servicios propios. En definitiva, favorecer la libre competencia en el ámbito de Internet.

[23] Para este apartado hemos encontrado de mucha utilidad el Manifiesto Digital de Telefónica (Steck C. *et al.*, 2014).

La existencia de una saludable competencia de mercado es un componente frecuente en las discusiones sobre neutralidad de la Red. Los prestadores de servicios de Internet entienden que la competencia en el mercado es útil, dado que ofrece a los consumidores la posibilidad de elección y fomenta la innovación entre los proveedores de servicios. Además, la promoción de la competencia para la provisión de acceso a Internet hace posible que los usuarios escojan entre diferentes servicios y experiencias en línea.

Por otro lado, no hay que olvidar que el tema de la neutralidad en la Red es mucho más amplio que el debate alrededor del comportamiento de los operadores de telecomunicación. Si el acceso a los contenidos de Internet debe ser igual para cualquier ciudadano, no debemos olvidar algunos comportamientos de las empresas tecnológicas grandes (Google, Facebook), que "imponen" políticas de privacidad abusivas o gestionan la publicidad que recibimos de una forma que dista mucho de ser respetuosa con los derechos de las personas.

2.3. El derecho a la educación

El derecho a la educación aparece recogido en el artículo 26.3 de la Declaración Universal de Derechos Humanos, en el artículo 13.3 del Pacto Internacional de Derechos Económicos, Sociales y Culturales, en el artículo 18.4 del Pacto Internacional de Derechos Civiles y Políticos, y en el Protocolo Adicional 1º, de 20 de marzo de 1952, al Convenio Europeo de Derechos Humanos de 1950. Los derechos integrados en el derecho a la educación son dos: el derecho a la educación y la libertad de enseñanza. El contenido esencial de ambos derechos consiste en **facilitar la educación a todo el mundo en condiciones de igualdad y admitir el mayor pluralismo posible**, tanto en la vertiente de derecho de prestación como en la vertiente de derecho de libertad.

El derecho a la educación constituye un derecho fundamental de naturaleza prestacional que aparece consagrado en la mayoría de los textos como un derecho **gratuito y obligatorio**, cuya implementación constituye una exigencia del poder público por medio de todas aquellas acciones y prestaciones que satisfagan los contenidos constitucionales del derecho. Dentro de los cometidos atribuidos al

Estado social destaca como prioritaria la **promoción de la igualdad** en la educación y la eliminación de los obstáculos que la impidan. La **educación ha de ser pública e igualitaria,** extenderse a todos los estratos sociales, **obligatoria y gozar de financiación pública.** Al Estado, junto con las Comunidades Autónomas, corresponde establecer los instrumentos materiales que han de permitir adquirir los conocimientos propios que capaciten a la persona para ir progresando en los diferentes niveles educativos, hasta llegar a adquirir los conocimientos necesarios para desempeñar una profesión.

Por otro lado, el derecho a la educación presenta una característica peculiar frente al resto de los derechos, pues, pese a ser un derecho fundamental, su titular no puede decidir ni la finalidad ni el contenido del mismo, ya que la finalidad viene recogida en la Constitución, y el contenido lo determina el legislador ordinario. En efecto, el artículo 27.2 CE señala que la finalidad de la educación es alcanzar el pleno desarrollo de la personalidad humana en el respeto a los principios democráticos de convivencia y de los derechos fundamentales. Por tanto, se trata de un proceso de instrucción y formación orientado a una finalidad ya determinada y que por ello condiciona la intervención del poder público en lo que a la educación se refiere. Será el legislador el que proyectará las grandes directrices contenidas en la Constitución en las leyes educativas que en cada momento social sean necesarias para conseguir el pleno desarrollo de la personalidad humana. Así, la Ley Orgánica 2/2006, de 3 de mayo, de Educación[24] (LOE), cuyos artículos 2 y 3 completan la redacción del artículo 2 de la LODE. En concreto la ley señala como principios que ha de conseguir el sistema educativo los siguientes: "A) el pleno desarrollo de la personalidad del alumno; B) **la formación en el respeto de los derechos y libertades fundamentales y en el ejercicio de la tolerancia y de la libertad dentro de los principios democráticos de convivencia;** C) **la adquisición de hábitos intelectuales y técnicos de trabajo, así como de conocimientos científicos, técnicos, humanísticos, históricos y estéticos;** D) **la capacitación para el ejercicio de actividades profesionales**; E) la formación en el respeto de la pluralidad lingüística y cultural de España; F) **la preparación para participar activamente en**

[24] BOE núm. 106, de 4 de mayo, de 2006.

la vida social y cultural; G) **la formación para la paz, la cooperación y la solidaridad entre los pueblos**."

Resulta absolutamente obvio que la formación en contenidos digitales y en utilización de tecnologías de la información forma parte de los principios a alcanzar por el sistema educativo.

El contenido integrado en el derecho a la educación que puede verse afectado de modo significativo por la sociedad digital es el cometido de diseñar los planes de estudio, y de facilitar el acceso gratuito a los medios educativos, intervenido todo por el principio de no discriminación[25]. Y es el Estado quien ha de proveer a los centros educativos de los elementos necesarios para dotar al derecho a la educación de la vertiente digital que demanda la sociedad actual. En el momento presente, el sistema educativo ha de dar respuesta a los retos que plantea la sociedad digital, con dos premisas que han acompañado a la educación en los diferentes momentos de la historia y que gozan de absoluta vigencia: **conseguir una educación sin discriminación y alcanzar una formación de calidad en todos los niveles.**

La presencia de la sociedad digital en la educación obliga a tener en cuenta las siguientes consideraciones:

- **Favorecer la educación digital de los ciudadanos**, en los diferentes niveles educativos, incorporando materias con contenidos que permitan a los alumnos/as adquirir las capacidades y habilidades necesarias para la utilización adecuada y útil de Internet. Esta obligación del poder público responde a la naturaleza prestacional del derecho a la educación, cuyos

[25] Como se contempla en la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores, constituida en el seno de la Comisión conjunta de las Comisiones de Interior, de Educación y Deporte y de Industria, Energía y Turismo: "Internet (es) 'la gran ciudad del siglo XXI', una ciudad basada en el uso intensivo de las tecnologías de la información y la comunicación, global, abierta y en cambio permanente, constituyendo el reto de integrar la escuela (en sí mismo "la tecnología más potente que ha desarrollado la humanidad para alcanzar cotas más altas de justicia y prosperidad") con las posibilidades de aprendizaje que ofrecen las nuevas tecnologías, puestas al servicio tanto de los niños (en condiciones de igualdad, para que nadie quede al margen de la adquisición de las competencias básicas digitales, e integrando a quienes tienen inteligencias distintas, a veces las más creativas) como de los profesores ("el gran descubrimiento de la transformación educativa"), para los que, como señaló Ana María Román, aquellas constituyen un recurso clave en la dirección de la mejora de la calidad educativa, al permitir fomentar una cultura colaborativa y abierta en el entorno escolar, facilitar la educación personalizada y, en general, apoyar la tarea de mediación en la transmisión del conocimiento y en el interés por el mismo". Disponible en http://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_D_10_410_2763.PDF, p. 20.

contenidos ahora han de adecuarse a las exigencias del siglo XXI. El poder público, como sujeto responsable de la educación como servicio público, está obligado a diseñar y construir el sistema educativo dentro de los fines y principios de la educación, aunque la educación exige un compromiso por parte de los integrantes de la comunidad escolar, y también por el conjunto de la sociedad. Por supuesto los fines y los principios propios de la educación no pueden ser diferentes de los fines y principios democráticos y su objetivo la formación integral de la persona. Por lo que respecta a los planes de estudio, el poder público ha de incorporar asignaturas cuyos contenidos incluyan una formación completa en tecnologías, tanto en materias obligatorias como optativas. Tal y como señala la exposición de motivo de la LOE, "A la vista de la evolución acelerada de la ciencia y la tecnología y el impacto que dicha evolución tiene en el desarrollo social, es más necesario que nunca que la educación prepare adecuadamente para vivir en la nueva sociedad del conocimiento y poder afrontar los retos que de ello se derivan".

- Pero ello obliga también a un **uso racional y respetuoso de Internet**, acorde con la finalidad educativa de formación integral de la personalidad humana en el respeto a los principios democráticos y a los derechos de los ciudadanos. Hay que educar en el uso de Internet, e inculcar valores como el silencio y la desconexión[26]. Este uso es especialmente necesario en el ámbito educativo y en relación con los menores[27]. La utilización de Internet y la posibilidad de interactividad, esto es, la posibilidad de crear contenidos y compartirlos con otros usuarios a través de las redes sociales[28], obliga a insistir en una formación que enseñe al menor a utilizar estas herramientas y a no quedar desprotegido frente a ellas, protección que, además, ha de lograrse por los medios jurídicos apropiados. Ese espacio de creatividad de contenidos se traduce en el concepto de Web 2.0 en la que el usuario recibe la información que suministra la Red y se convierte también al mismo tiempo

[26] Ponencia conjunta de estudio…, *ob. cit.*, p. 24.

[27] En este sentido se puede ver la Ponencia conjunta de estudio…, *ob. cit.*, p. 25 y ss.

[28] El Instituto Nacional de Tecnologías de la Comunicación (INTECO) y la Agencia Española de Protección de Datos (AEPD) definieron en un estudio de 2009 las redes sociales online como "servicios prestados a través de Internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles" (INTECO/AEPD, *Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online*, 2009).

en creador de contenidos (Heredero Higueras). Existen propuestas para limitar a través de medidas técnicas los contenidos no adecuados para los menores, como una medida más de protección (Roig Batalla), pues los contenidos no aparecen restringidos por el factor tiempo, ya que están disponibles siempre. No hablamos solamente de contenidos ilícitos (pornografía infantil, páginas que incitan al odio, al racismo, etc.), sino de contenidos lícitos pero desaconsejables para los menores, como páginas que enseñan prácticas como la anorexia, o como falsificar DNI, entradas para conciertos, etc.). Internet combina el binomio oportunidades y riesgos y la educación ha de potenciar lo primero y conjurar lo segundo. La educación en medios tiene que rescatar los valores positivos de la Red. La Red significa "diálogo, intercambio de puntos de vista, búsqueda de acuerdo y de consenso, aspiración al flujo igualitario de información, la abolición de diferencias de clase y de estatus", entre otros muchos valores. La educación en medios "ha de construir un sentido de la realidad centrado en la libertad y en la dignidad humana" (Pérez Tornero 2005: 255).

- También hay que recordar la obligación que recoge la LOE en su apartado 3 i), sobre la enseñanza de las personas adultas, como uno de los tipos de enseñanza del sistema educativo. Las personas adultas constituyen un grupo que será necesario tener en cuenta en lo que a formación tecnológica se refiere si no queremos incluirlos en la brecha digital.
- El **acceso a los contenidos educativos** debe ser universal y gratuito, o con tarifas razonables, y debe garantizarse la igualdad de oportunidades, sin que pueda provocarse una brecha digital. Se trata de aprovechar las ventajas de Internet para impartir los conocimientos educativos de las materias que así lo permitan (que todas lo permiten). Para ello, la implantación de los instrumentos técnicos y tecnológicos debe realizarse de una manera racional y sin discriminación entre centros urbanos y rurales, así como entre centros públicos y concertados. Ello exige, además de un esfuerzo de medios materiales y económicos por parte de las Administraciones implicadas, una aportación generosa de las empresas que oferten dichos servicios, con el fin de promover la extensión de los servicios a todos los ciudadanos en los centros escolares. En este sentido hay que recordar que el artículo 32.3 de la

> Ley de propiedad intelectual[29] (LPI) exime al personal de la educación reglada, de las Universidades y de Organismos Públicos de Investigación en su función científica de la "autorización del autor o editor para realizar actos de reproducción, distribución y comunicación pública de pequeños fragmentos de obras y de obras aisladas de carácter plástico o fotográfico figurativo, cuando, no concurriendo una finalidad comercial, se cumplan simultáneamente las siguientes condiciones", que detalla el precepto.

Como elementos para determinar una educación completa en los entornos digitales puede resultar orientativa la distinción entre los **riesgos de Internet y los riesgos en Internet**[30]. Los primeros son aquellos riesgos que van unidos a Internet de forma inseparable, mientras que los segundos son los riesgos que encuentran en Internet un medio idóneo para propagarse. Entre los primeros podemos señalar la forma en la que aprehendemos la información, el uso excesivo de Internet, la forma de relacionarnos con los demás. Entre los segundos podemos encontrar los riesgos de contenidos, como la pornografía infantil, y los riesgos de contacto, que pueden afectar a la integridad física o psíquica del menor como el *ciberbullying.*

Por otro lado, hay que tener en cuenta que, aun aceptando la diferente percepción que existe entre los educadores y los educandos en lo que a los riesgos en Internet se refiere, existen amenazas objetivas: la ciberdelincuencia y el riesgo sobre la intimidad de los menores y la protección de datos. La ciberdelincuencia es objeto de tipificación a través de las medidas penales específicas y la protección de datos dispone de leyes particulares para garantizar la protección del menor a través de sus datos de carácter personal. La protección de datos en el mundo digital ha evolucionado y ha originado el concepto de *identidad digital*, que ha de ser mostrada al menor como un bien con un importante valor que hay que proteger. Aunque casi nadie confía en la seguridad de los datos que son volcados en Internet, y el ciudadano encuentra insuficiente la información sobre el destino y uso de los datos de carácter personal, en raras ocasiones estos inconvenientes juegan como impedimento para la

[29] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, reformada a través de la Ley 23/2006, de 7 de julio y de la Ley 21/2014, de 4 de noviembre.

[30] Ponencia conjunta de estudio…, *ob. cit.*, p. 21.

entrega de los datos por parte del sujeto. Si hablamos de los menores, la entrega de los datos no se cuestiona, simplemente es aceptada como parte del mundo digital. Es más, los datos y la revelación de la identidad a través de las redes forma parte del nuevo sistema de relaciones sociales que entablan los menores. Aunque las relaciones "virtuales" son todavía complementarias de las "presenciales", y no parece racional pensar que puedan llegar a sustituirlas, aunque sí quizá a equipararlas cuantitativamente.

2.4. El derecho a la libertad de expresión y a la información

El derecho a la libertad de expresión se ha visto modificado en cuanto a las exigencias constitucionales de protección de este derecho en Internet, teniendo en cuenta que esta última resulta un instrumento que permite volcar la opinión subjetiva de una manera fácil, rápida y con una capacidad de transmisión casi infinita. De "plaza pública" o "ágora de la comunidad global" aparece calificada Internet[31]. En este sentido se presentan problemas de protección de la propiedad intelectual, y de límites y de mecanismos de protección frente a ataques a la libertad de expresión. Desde otro punto de vista se plantea el control de las extralimitaciones de la libertad de expresión cuando se vierten en Internet contenidos irrespetuosos con los límites constitucionales de la libertad de expresión.

El ejercicio de la libertad de expresión a través de Internet tendrá lugar en aquellas páginas dedicadas a la "difusión de información" (con independencia de generar beneficio) o , en terminología de la LSSICE, al suministro de información vía electrónica "(como el que efectúan los periódicos o revistas que pueden encontrarse en la red)", así como en "las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de Información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio…), siempre que

[31] Informe Final de la Comisión Especial sobre Redes Informáticas del Senado español, aprobado el 9 de diciembre de 1999, disponible en http://www.senado.es/pdf/legis6/senado/bocg/I0812.PDF

represente una actividad económica para el prestador". Por tanto la libertad de expresión resulta amparable en **las páginas que suministran información,** pues recogen contenidos que proyectan ideas o pensamientos que han de ser libres en un Estado democrático, pensamos en los periódicos y revistas digitales, pero también en **los servicios de intermediación**, así como las páginas web de particulares.

Veamos cómo queda afectada la libertad de expresión en relación con Internet. El artículo 8 de la LSSICE enumera un conjunto de principios que han de ser respetados por los servicios de la sociedad de la información[32]. Para garantizar dicha protección, la norma faculta a los órganos competentes en el ejercicio de sus funciones a adoptar las medidas necesarias. Las medidas necesarias con dos finalidades, a tenor del propio precepto: interrumpir la prestación de los servicios o bien retirar los datos que vulneren los principios a que alude el artículo. Ahora bien, la adopción y cumplimiento de las medidas de restricción que recoge el artículos no son absolutas, sino que habrán de respetar, en todo caso "las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados. En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, solo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto que garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información". Luego la protección de la libertad de expresión puede jugar como límite a la retirada de contenidos en Internet. Ahora bien, el "órgano competente" para llevar a cabo las medidas limitativas de la sociedad de la información en el momento en el que pudiera verse afectada la libertad de expresión, solamente puede ser el órgano judicial, único órgano competente para llevar a cabo una actuación en el campo de los derechos fundamentales, tal y como refleja el artículo 20.3 de la CE en relación

[32] Los principios a que alude el apartado son: "a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional; b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores; c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social; d) La protección de la juventud y de la infancia; y e) La salvaguarda de los derechos de propiedad intelectual".

con la libertad de expresión, según el cual, solo por medio de resolución judicial podrá acordarse el secuestro de publicaciones, grabaciones o cualquier otro medio de información, expresión que permitiría incluir la información vía Internet. No cabe realizar otra interpretación posible en el contexto de la libertad de expresión, con lo que la posible imprecisión del precepto de la LSSICE, al menos en lo que respecta a este derecho fundamental, queda eliminada.

El **derecho a la información** consiste en el derecho a ser informado sin que el Estado pueda manipular información que los ciudadanos tienen derecho a conocer, al tiempo que ha de impedir que nadie pueda llegar a hacerlo[33]. Además, supone la libertad de dar a conocer a la opinión pública información veraz, libre, efectiva, objetiva y plural. La veracidad está establecida con claridad por el Tribunal Constitucional (STC 223/1992 y 47/2002). El hecho de que la información sea de interés general también ha sido determinado por STC 57/1999.

Estos derechos no son absolutos, y colisionan con frecuencia, entre sí y con otros (derecho al honor, intimidad, propia imagen). Así, el derecho a la información no existe si las compañías proveedoras monitorizan nuestra actividad online. En cierta forma este hecho amenaza la libertad de expresión: la presión voluntaria autoimpuesta por las empresas, que vigilan lo que se publica o no desde su servicio, y censuran a sus ciudadanos. La intervención de los gobiernos, regulando el derecho al olvido de forma que se puede afectar muy fácilmente a la libertad de información, cuando entran en conflicto. La técnica "curarse en salud", esto es, ante la posibilidad de verse sancionado con cuantiosas multas, con responsabilidades en materia de protección de datos, pueden eliminar contenidos simplemente para evitarse problemas. Las medidas adoptadas para proteger el *copyright* han sido uno de los mayores enemigos de la libertad de expresión e información online.

También pueden existir conflictos entre el derecho al olvido y la libertad de expresión. En este caso, el nuevo reglamento trata de ordenar esta cuestión y evitar ese conflicto. Contribuye a un ecosistema más saludable, evita ir en contra de la libertad de expresión. Esto no significa que su interpretación en las diferentes

[33] Goig Martínez, J.M., Núñez Matínez, M.A., Núñez Rivero, C. (2006:274).

jurisdicciones sí pueda hacer que se vea vulnerada la libertad de expresión. Se debe diferenciar ente lo que es legal y procede derecho al olvido si es difamatorio, o si es ilegal y simplemente hay que eliminarlo por este hecho. El derecho a la privacidad es inherente a la libertad de expresión y viceversa, se necesitan mutuamente. Los contenidos difamatorios son el elemento que ordena y fija el punto de partida hacia ese equilibrio.

Internet consiste fundamentalmente en un conjunto de "contenidos", pero a la mayor parte de los usuarios no les preocupa cómo se elaboran esos contenidos, las noticias en concreto. Debemos preocuparnos porque éstos quieran entender, que quieran conocer o comprender los riesgos. Existen filtros técnicos que permiten seleccionar las noticias, tanto verdaderas como falsas. Los algoritmos deben ayudar a que los usuarios puedan detectar esa diferencia. Pero es más importante tratar de fomentar una mayor verdad, y detectar el problema de la información falsa.

Internet han justificado una regulación muy diferente en este medio si lo comparamos con la que se aplica al mundo editorial tradicional. En éste, las editoriales responden por los contenidos que publican. Sin embargo, en Internet los prestadores de servicios (por ejemplo, los que alojan contenidos de cualquier índole en la Web, como un blog), no responden de los contenidos sino hasta que un órgano competente declare la ilicitud de los mismos y ordene la retirada. Parece que esta norma, que deja un margen muy amplio para la libertad de expresión y de información, tiene su justificación en el hecho de que el responsable de una web, por ejemplo, no podría físicamente controlar los contenidos que se publican debido a la cantidad de los mismos, debido a la naturaleza que tiene Internet.

Por otro lado, los gobiernos deben impulsar políticas de transparencia[34] también para empresas, pues obtendrían el beneficio de ganarse la confianza del usuario. En todo caso, la transparencia es un punto de partida no un fin en sí mismo.

[34] Guichot E. (2011).

2.5. El derecho de asociación y participación

El derecho de asociación se ve afectado por los mecanismos que permite Internet para poder formar parte de una asociación. El derecho de asociación está regulado en la Ley Orgánica 1/2002, de 22 de marzo, reguladora del derecho de asociación[35]. La única especialidad que permite la creación de una asociación online es la posibilidad de mantener todos los elementos propios del derecho fundamental protegidos en la Red. Se debe ser especialmente cuidadoso en relación con los datos de carácter personal. Se han de observar los principios de calidad de los datos del artículo 4 de la LOPD, cuando se soliciten datos del sujeto que desea formar parte de la asociación, así como de los propios asociados. Se deben garantizar los derechos de acceso, rectificación y particularmente el derecho de cancelación o supresión (derecho al olvido del art. 17 RGPD), cuando el asociado manifieste su deseo de dejar de pertenecer a la asociación, derecho que forma parte del derecho fundamental de asociación y por tanto debe rodearse de las garantías constitucionales necesarias para hacerlo efectivo, también vía telemática. El derecho de cancelación de los datos ha de ser ejercido por el asociado y observado con todas las garantías previstas en las leyes.

En el ejercicio del derecho de asociación vía Internet adquieren relevancia el derecho a la portabilidad de los datos, que permite al sujeto llevarse sus datos de carácter personal entregados a la asociación y comunicarlos a otro responsable.

2.6. El derecho a la identidad online y a la protección del anonimato

Toda persona tiene asociado un determinado perfil online que el sujeto mismo ha elaborado mediante la incorporación, modificación o borrado de datos, comentarios, etc. A través de la Red desvelamos lo que somos, pensamos, es decir, ofrecemos un dibujo de nuestra personalidad, según nuestras propias palabras o actividad en la Red. En la sociedad analógica nuestra forma de ser se revela a través de nuestras acciones, de nuestro modo de comportarnos, etc. En la Red, el perfil del sujeto se revela al mundo digital a través de su participación en los diferentes instrumentos que ofrece Internet. “La identidad digital es la expresión electrónica del conjunto de

[35] BOE núm. 73, de 26 de marzo, de 2002.

rasgos con los que una persona física o jurídica, se individualiza frente a los demás" (Fernández Burgueño, 2012:127). Son atributos identificativos de la persona, por lo que esa información constituye datos de carácter personal a los que les sería de aplicación la LOPD.

Pero la **identidad digital** no solamente se construye a través de la información que el sujeto vuelca sobre sí mismo, sino también por medio del perfil que los terceros pueden ir elaborando a partir de dicha información. Por ello la identidad digital se va construyendo desde todos los contenidos e informaciones que sobre un sujeto existen en Internet, lo que incluye tanto los contenidos generados por él mismo como los generados por los demás usuarios, aunque estos contenidos subjetivos constituyen más propiamente dicho la **reputación online.** Estas opiniones sobre aspectos de nuestra personalidad compartidos en Internet por terceros, dan lugar a la imagen online que los demás tienen de nosotros. Por tanto, la identidad es la imagen que el sujeto quiere dar de sí mismo, construida con mayor o menor esfuerzo y la interpretación de dicha identidad es la reputación (Fernández Burgueño 2012: 128). La reputación online tendría su equivalente en el mundo analógico en el derecho al honor del artículo 18.1 de la CE, que protege el reconocimiento que los demás tienen de nosotros mismos, la consideración ajena, la estima, el buen nombre.

Los elementos que construyen tanto la identidad como la reputación online son comunes, por ejemplo: comentarios en un blog, en foros, en Youtube, perfiles, tanto personales como profesionales en Facebook, Tuenti, Twitter, Linkedin, etc., imágenes, actividad laboral, como por ejemplo, oposiciones a las que la persona se ha presentado, trabajos subidos a la Red, vídeos, actos de ocio a los que se ha asistido, conciertos, fiestas, etc.

El **derecho a la identidad online** o **identidad digital** es el derecho a disponer de la identidad online o perfil, pudiendo el sujeto ejercer un control sobre las informaciones que él mismo ha subido a la Red, para modificarlas o suprimirlas. Una de las dificultades con las que se encuentra el ejercicio del derecho a la identidad es la accesibilidad universal a los contenidos que permite Internet, lo que dificulta el control de la posesión y conocimiento de dicha información y su efecto de

autenticidad y fiabilidad, aspectos estos últimos que pueden ser más difícilmente verificables, por formar parte de las informaciones que los demás hacen sobre nosotros. Además de los efectos señalados, la permanencia de los datos en la Red es inimaginable y, junto a la permanencia, la posibilidad de replicar los contenidos de forma prácticamente infinita dificulta el control de la identidad digital por parte del sujeto (Fernández Burgueño, 2012:131). El derecho al olvido permite borrar los datos que forman parte de la identidad online, y los que conforman nuestra reputación, obligando a la persona responsable del tratamiento a su supresión, con el fin de que pueda impedirse la búsqueda de los datos a través de los buscadores, derecho del que ya hemos hablado.

Para la construcción de una identidad online que no pueda provocar más adelante agravios en los derechos de los sujetos, es necesario educar en la elaboración de contenidos propios responsables y prudentes, así como ejercer esa responsabilidad y prudencia para analizar y comentar los perfiles de los demás sujetos. Dado que en la Red es muy difícil borrar perfiles, salvo el ejercicio del derecho al olvido ante los responsables de los tratamientos de datos, la prevención es la mejor manera de evitar un daño en la personalidad del sujeto al construirse su identidad online, algo que hoy parece ya irrenunciable.

Por otro lado, la identidad online y la reputación online no son exclusivas de las personas físicas. Las personas jurídicas pueden crearse un perfil en la Red, una determinada identidad que sirva para su proyección comercial y la reputación online se construye a partir de los comentarios de los clientes.

El **derecho a proteger el anonimato** es el derecho de toda persona a utilizar Internet protegiendo su identidad, por medio de procedimientos e instrumentos técnicos o bien, el derecho a salvaguardar un cierto anonimato mientras se interactúa en la Red. El derecho a proteger el anonimato en Internet no tendría por qué justificarse, debería bastar con un acto de voluntad del sujeto, en el sentido de no querer entregar datos de carácter personal que le identifiquen o le puedan identificar, siempre que no sea obligatoria su entrega, o de navegar por Internet sin dejar rastro, pues el recorrido realizado visitando determinadas páginas web puede ofrecer un perfil de la persona

que pueda permitir su identificación. Toda modalidad de acceso a Internet debería tender a garantizar a la persona el anonimato en la Red, sin que esta posibilidad significare una disminución en los accesos, servicios o posibilidades en Internet. El sujeto tampoco podrá sufrir ninguna discriminación por su deseo de navegar en Internet manteniendo oculta su identidad. El anonimato en la Red puede significar un importante elemento de garantía de la libertad de la persona, aunque como todo instrumento de garantía no puede tener carácter absoluto y ha de tener limitaciones basadas en la protección de intereses públicos relevantes, o los derechos y libertades de un tercero, o medidas que fueran proporcionadas en una sociedad democrática y ajustadas a la ley.

El derecho a mantener el anonimato en la Red es objeto de polémica, especialmente cuando a través del anonimato y en el ejercicio de la libertad de expresión en la Red se puede producir una lesión en el derecho al honor de un tercero. Bajo el anonimato no pueden verterse mensajes ofensivos, o insultantes, o lesivos para el derecho al honor. El TEDH (asunto Delfi AS. c Estonia 64569/09) ha sentenciado que un mensaje ofensivo o insultante difundido anónimamente (o con identificación) no puede quedar impune en la Red, por lo que la responsabilidad por el mismo se traslada al titular del portal en el que se ha difundido el mensaje. La sentencia señala que la Red permite difundir comentarios anónimos, lo que eleva la facilidad y por tanto el riesgo de lesionar el derecho al honor a través de Internet. La dificultad de responsabilizar a los autores de dichos comentarios obliga al TEDH a trasladar dicha responsabilidad al responsable del portal a través del cual se difunden. La transmisión de dicha responsabilidad se justifica como medida de protección del derecho al honor frente a la libertad de expresión. El TEDH entiende que los comentarios vertidos en Internet en un medio digital han de ser evaluados por el responsable del medio y, cuando dichos comentarios puedan dañar el honor de la persona o provocar una avalancha de comentarios perjudiciales, debe llevar a cabo su retirada. En el caso analizado, el TEDH entiende que el medio digital debió actuar con diligencia y prever los riesgos que la publicación podía ocasionar, al no hacerlo así, actúo con irresponsabilidad. Por otro lado, la parte ofendida por los comentarios difundidos en la Red no puede demandar a todos los que vertieron comentarios en el medio pues, es un número elevado de personas y algunas de ellas han participado de

forma anónima. Si se obligara a la persona perjudicada a emprender este tipo de acciones se estaría vulnerando su derecho a la tutela judicial efectiva, pues implicaría prácticamente demandar a todos los implicados. Por ello, como el control por Internet no puede soportarlo solamente una persona, corresponde al operador de una portal de noticias adoptar las medidas necesarias para evitar que la Red sirva como instrumento para vulnerar los derechos de la personalidad de los sujetos. En definitiva, el medio digital (los prestadores de servicios de intermediación) debe disponer de herramientas suficientes para retirar los mensajes ofensivos, difamatorios y lesivos para el derecho al honor de las personas, lo que a todas luces puede constituir una restricción a la libertad de expresión.

Pueden arbitrarse sistemas que detecten y retiren de forma automática comentarios que incluyan algunas palabras injuriosas u ofensivas, o bien contemplar la retirada de mensajes de semejante contenido tras la advertencia por parte de la víctima o de otro usuario, aunque tales herramientas pueden ser consideradas como insuficientes y poco diligentes para eximir al responsable del medio de responsabilidad.

La dificultad ha estribado en determinar la responsabilidad de los intermediarios en la Directiva 2000/31/CE, sobre el comercio electrónico, es decir, si el prestador del servicio (titular del sitio web, portal, blog…) puede o no ser considerado un intermediario con respecto a los contenidos para valorar si tiene conocimiento de que la actividad es ilícita y puede actuar para retirar los comentarios o impedir el acceso a ellos, ya que la Directiva exoneraba de responsabilidad a los prestadores de servicios frente a estas situaciones y en los artículos 13 y ss. de la LSSICE quedan exonerados de responsabilidad.

En relación a la conservación de datos de los usuarios que puede afectar a la intimidad del sujeto y a la protección de datos hay que referirse a la Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[36], determinaba la conservación de los datos con fines de investigación,

[36] DOUE L 105, de 13 de abril de 2006.

detección y enjuiciamiento de los delitos graves, tal y como se definen en la legislación nacional de cada Estado miembro. La Directiva se aplicaba a los datos de tráfico y de localización de datos de personas físicas y jurídicas y a los datos necesarios para poder identificar al abonado o al usuario registrado (art. 2). El artículo 5 detallaba todas las categorías de datos que deben ser conservados y el artículo 6 fijaba un periodo de conservación entre seis meses como mínimo y dos años máximo, a partir de la fecha de comunicación[37]. Sin embargo, la STJUE de 8 de abril de 2014, declaraba inválida la Directiva 2006/24/CE, pues considera que la conservación de los datos constituye una vulneración del artículo 7 de la CEDH, relativo a la vida privada y del artículo 8, sobre la protección de los datos de carácter personal.

En cumplimiento de dicha Directiva, el legislador español elaboró la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas[38] (la disposición derogatoria única deroga el artículo 12 de la LSSICE que regulaba la conservación de los datos) y, aunque la invalidez de la Directiva no suponga de manera automática la anulación de la legislación nacional de desarrollo de la misma, habrá que examinar con precisión la regulación de la ley interna para ver en qué medida queda invalidada por la sentencia del Tribunal europeo. Serán los órganos judiciales los encargados de valorar en cada caso la aplicación de la ley y su adecuación a la STJUE. Aunque no sea este el lugar para proceder a un examen a fondo de la adecuación de la norma española a la Directiva invalidada, algunos argumentos de análisis se pueden aportar.

[37] La Directiva justifica la necesidad de levantar dicho anonimato, que es en definitiva lo que significa la conservación de los datos pese a reconocer que " de conformidad con el art. 8 CEDH garantiza el derecho de toda persona al respeto a su vida privada y su correspondencia y que las injerencias públicas al ejercicio de dicho derecho deben estar previstas por la ley y constituir una medida que, en una sociedad democrática sea necesaria, entre otros asuntos, para la seguridad ya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros. Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva. Por consiguiente, la adopción de un instrumento de conservación de datos que cumpla los requisitos del artículo 8 del CEDH es una medida necesaria." (considerando 9).

[38] BOE núm. 251, de 19 de octubre de 2007.

El artículo 3 de la Ley 25/2007 detalla los datos objeto de conservación que el precepto agrupa en:

a) Datos necesarios para rastrear e identificar el origen de una comunicación: en primer lugar con respecto a la telefonía de red fija y a la telefonía de red móvil y, en segundo lugar, con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet.

b) Datos necesarios para identificar el destino de una comunicación: tanto con respecto a la telefonía de red fija y a la telefonía de red móvil como respecto al correo electrónico por Internet y la telefonía por Internet.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación, también con respecto a la telefonía de red fija y de red móvil y con respecto a Internet, el correo electrónico por Internet y a la telefonía por Internet.

d) Datos necesarios para identificar el tipo de comunicación, con respecto a la telefonía de red fija y de red móvil y respecto al correo electrónico por Internet y a la telefonía por Internet.

e) Datos necesario para identificar el equipo de comunicación de los usuarios o lo que se considere equipo de comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil.

El artículo 1 de la Ley 25/2007 establece "la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de las correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales". La norma se aplica a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

La STJUE citada señalaba que los datos conservados y en las condiciones que señalaba la Directiva pueden proporcionar información muy precisa sobre la vida

privada de las personas cuyos datos se conserven, con el desconocimiento de ello por parte del usuario registrado o abonado. El TJUE entiende que el fin de la Directiva de luchar contra la delincuencia, el terrorismo, en definitiva garantizar el interés general y la seguridad pública, son medidas que pueden justificar una limitación del derecho a la vida privada y a la protección de datos, si bien en la defensa de dichos argumentos, el legislador europeo ha sobrepasado el principio de proporcionalidad. Los datos cuya conservación permite la Directiva, que coinciden con los que se detallan en el artículo 3 de la Ley 25/2007, "pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyo datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan" (párr. 27). El Tribunal Europeo entiende que la injerencia que supone la conservación de esos datos no constituye una vulneración en los derechos a la vida privada y a la protección de datos. En el primer caso porque no se accede al contenido de la comunicación y en el segundo porque la Directiva establece el sometimiento de los proveedores de servicios de comunicaciones electrónicas a los principios de la protección de datos, y la adopción de medidas técnicas que velen por la conservación de los datos. La conservación de los datos se vincula a los fines de investigación, detección y enjuiciamiento de delitos graves, lo que constituye un objetivo de interés general. Sin embargo, el TJUE concluye que la Directiva no recoge reglas claras y precisas que reduzcan la gravedad de la injerencia en los artículos 7 y 8 del CEDH y limiten dicha injerencia a lo estrictamente necesario. Tampoco las medidas de protección de los datos que contempla la Directiva resultan lo suficientemente precisas y adaptadas a la gran cantidad de datos cuya conservación permite la Directiva, "al carácter sensible de estos datos y al riesgo de acceso ilícito a ello", y tampoco se desprende un obligación concreta para los Estados miembros para establecer dichas reglas. La Directiva adolece igualmente de límites que puedan evitar que las autoridades nacionales utilicen los datos conservados solamente a efectos de seguridad e interés general. La carencia de un control judicial previo de acceso a los datos tampoco se contempla. Por lo demás, el periodo de conservación de los datos, de seis meses a veinticuatro meses, sin ningún criterio objetivo para el mismo tampoco constituye

una garantía. Por todo lo analizado, el TEJU determina la invalidez de la norma europea.

La Ley 25/2007, de 18 de octubre, recoge los requisitos para la cesión de los datos conservados, esto es, los fines que determinen la propia norma y la previa autorización judicial (art. 6), que constituye, especialmente este último, un requisito reclamado por la STJUE. En cuanto a los fines de la ley española, el artículo 1 habla de detección, investigación y enjuiciamiento de los delitos graves contemplados en el Código Penal o en leyes penales especiales. La LECr (art. 588 ter) señala que "la autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.71 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación", lo que ha pasado de permitir la averiguación de la identidad de quien realiza la comunicación solamente para los delitos graves a prácticamente todo delito, incluidos aquellos que se cometan vía Internet. La alusión a los delitos graves del Código Penal, que según el artículo 13.4 son aquellos delitos castigados con pena grave y con pena menos grave, parece quedar más delimitada en el ordenamiento español. En nuestra opinión la Ley 25/2007, es una trasposición casi literal de la Directiva invalidada, aunque mejora las garantías de conservación de los datos. El debate sigue abierto, ya que parte de la doctrina entiende que la conservación masiva de datos constituye una vulneración del derecho a la vida privada y a la protección de datos de los artículos 7 y 8 del CEDH. Otra parte entiende que la ley española es acorde con la legislación de protección de datos. El TJUE parece zanjar el debate señalando, en la sentencia de 21 de diciembre de 2016 (Asuntos c-203/15 y C-698/15) (DOUE C 53 de 20.2.2017), que "el artículo 15 de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2005, en relación con los artículos 7, 8, 11 y 52, apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que se opone a una normativa estatal que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos

los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica".

El TJUE se opone en esta sentencia de 2016 a que una norma nacional permita "una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica, (…) en particular el acceso a las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano judicial o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión". Por el contrario, dice la sentencia, "el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido" (fto. jco. 108).

Por tanto, cabe señalar que la norma interna que regula la conservación de los datos de forma indiscriminada atenta contra el derecho a la vida privada y la protección de datos personales, constituyendo una injerencia desproporcionada y no justificada en los mismos y por tanto la ley española es contraria el Derecho de la Unión, al no respetar los requisitos y garantías que señala la STJUE de 8 de abril de 2014 en relación con la protección de los artículos 7 y 8 de la CEDH y permitir una conservación generalizada de datos.

2.7. El derecho a la desconexión digital

La desconexión digital laboral o el derecho a la desconexión laboral es el derecho de los trabajadores a desconectar del trabajo por medios digitales una vez finalizada la jornada laboral convenida. Este derecho se configura como un derecho negativo, de

no hacer, persiguiendo el Derecho con su regulación amparar una actitud de abstención de la persona en relación con el ámbito laboral, a través de medios tecnológicos y en determinadas condiciones, sin que esa abstención de trabajar pueda ser sancionada por incumplimiento de las obligaciones laborales. La regulación del derecho a la desconexión laboral guarda relación con dos elementos básicos de las relaciones de trabajo: la jornada laboral y el lugar de trabajo, elementos que han experimentado una profunda transformación con los medios digitales y que debido a ello requieren una revisión.

El contenido del derecho comprendería:

- el derecho a no recibir correos electrónicos tras la jornada laboral,
- el derecho a no conectarse a Internet para cuestiones laborales, por medio de *tablets*, *smartphones*, información en la nube, etc.

La implantación y extensión de los medios tecnológicos ha supuesto un elemento de desarrollo importante para las empresas, pues fomentan la productividad, y con ello los ingresos y la investigación e innovación[39], y facilitan la flexibilidad de la jornada laboral. Pero también, con la presencia de las TIC se corre el riesgo de una conexión permanente a cuestiones laborales que iría en contra del concepto de trabajo como derecho y como deber, podría provocar problemas de salud, como estrés, dependencia, adicción, etc., alterar el desarrollo de la vida personal y familiar y por tanto de la personalidad. En el ámbito laboral, la permanente conexión digital alarga la jornada laboral más allá de los límites legales establecidos, pudiendo transformarse en ininterrumpida, lo que puede provocar estrés y vulnerar el derecho al descanso. Igualmente, una atención permanente a las comunicaciones digitales de la empresa por parte del trabajador puede lesionar el derecho a la intimidad personal y familiar del artículo 18.1 de la CE en el ámbito domiciliario.

El derecho a la desconexión digital obliga a reflexionar acerca de algunos de los elementos que integran el mundo laboral, como la jornada de trabajo y el puesto de trabajo. El artículo 34 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el

[39] Informe de Kelevra, *El impacto de la Tecnología Móvil en las empresas,* disponible en http://kelevra.es/el-impacto-de-la-tecnologia-movil-en-las-empresas/

que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, señala que la jornada de trabajo será la jornada pactada en los convenios colectivos o contratos de trabajo, pero en ningún caso podrá superar el máximo de 40 horas semanales de trabajo efectivo en cómputo anual. Aunque la distribución de la jornada laboral puede ser irregular, la ley dice que a lo largo del año, habrá de respetar "los periodos mínimos de descanso diario y semanal previsto en la ley". El artículo 34.3 del ET señala que entre el final de una jornada y el comienzo de la siguiente deberá haber como mínimo un periodo de doce horas. Por otro lado, el número ordinario de horas de trabajo en una jornada no podrá ser superior a nueve horas diarias, salvo que por convenio se haya establecido otra cosa. A efectos del derecho a la observancia y regulación de la desconexión digital laboral los preceptos que debemos tener en cuenta son los que limitan las horas de trabajo diarias a nueve, salvo acuerdo contrario y el periodo mínimo de descanso entre jornadas, que será al menos de doce horas. Los intervalos delimitados por la ley determinan que, durante las doce horas de interrupción, el trabajador no podrá atenderse cuestiones de trabajo a través de medios digitales (ni de ninguna otra manera), y que, más allá de las nueve horas diarias de trabajo fijadas, tampoco existe obligación de mantener por medios digitales ninguna conexión con el ámbito del trabajo. Lo contrario determinaría la continuidad de la jornada laboral más allá del periodo establecido Por otro lado, la jornada laboral computa desde que comienza hasta que finaliza y estos tiempos se cuentan desde que el trabajador se encuentra en el puesto de trabajo (art. 34.5 ET). Junto a ello, el derecho a la desconexión digital laboral se ha de extender a las vacaciones y a los periodos de descanso semanal.

El derecho a la desconexión laboral altera parcialmente tanto el sentido de la jornada laboral como las circunstancias de comienzo y de fin de la misma, y el lugar de trabajo, pues la atención permanente a las conexiones digitales en el ámbito laboral pero ininterrumpida hace prácticamente imposible concretar los tiempos de conexión por motivos de trabajo y añadirlos al cómputo general de la jornada laboral. Por otro lado, el puesto de trabajo va unido al trabajador, en la medida en que tenga acceso vía Internet o vía *app* a cuestiones laborales, por lo que el concepto de lugar de trabajo se ve igualmente diluido.

El derecho a la desconexión laboral ha de construirse desde la perspectiva del reconocimiento del derecho en los convenios colectivos, como un derecho más del trabajador, y también en la legislación general, junto con la previsión de un sistema de garantías que lo protejan. Pero también ha de construirse desde la perspectiva de la obligación de la empresa de implantar medios técnicos que impidan mantener la comunicación con el trabajador más allá de la jornada laboral, que, por lo demás, puede contemplar los ajustes necesarios para permitir dicha conexión, además de la disponibilidad laboral, pero no más allá del tiempo estipulado legalmente.

En España, se ha redactado el primer convenio laboral que reconoce el derecho a la desconexión fuera del horario laboral[40], que ve modificado la idea de lugar de la prestación laboral y el tiempo de trabajo que, al poder ir inescindiblemente unidos al trabajador vía digital, pueden llegar a provocar injerencias en su derecho a la intimidad personal y familiar fuera y dentro del ámbito domiciliario, por lo que el derecho a la desconexión laboral es una garantía para el disfrute de aquellos derechos de la personalidad. Por otro lado, el convenio admite que la conexión laboral permanente puede provocar estrés. Por ello, el convenio citado reconoce que "salvo causa de fuerza mayor o circunstancias excepcionales AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo".

El convenio colectivo regula también el teletrabajo como una nueva forma de desempeñar la actividad laboral. El teletrabajo consiste en desarrollar la actividad laboral a distancia, fuera del lugar habitual de trabajo y por medio de las TIC. El teletrabajo es una forma de trabajo que mejora la conciliación de la vida laboral con la familiar. La empresa podrá acordar la modalidad de teletrabajo dependiendo del puesto desempeñado y siempre que no se altere la organización de la empresa que corresponde al empresario. El teletrabajo se podrá alternar con el trabajo desde el puesto de trabajo en la empresa.

[40] https://cincodias.elpais.com/cincodias/2017/07/20/midinero/1500549050_709216.html

En lo que a iniciativas legislativas se refiere, y siguiendo el ejemplo de la aprobación en Francia de la Ley que regula el derecho a la desconexión laboral[41], se ha presentado una proposición no de ley para instar al Gobierno a regular el derecho a la desconexión laboral[42]. La finalidad de la regulación, como reconoce la proposición no de Ley, es evitar que "los trabajadores y trabajadoras puedan continuar trabajando después de finalizar su jornada laboral utilizando los medios electrónicos de la empresa" (p. 10). La proposición no de Ley insta al Gobierno a:

> "1. Impulsar una regulación legal conjuntamente con los agentes sociales del uso de las tecnologías de la comunicación (mensajería y correos electrónicos o dispositivos móviles) fuera de la jornada laboral con el objetivo de evitar que los trabajadores y trabajadoras puedan continuar trabajando después de finalizar su jornada laboral utilizando los medios electrónicos de la empresa, y garantizar la seguridad y salud en el trabajo y el descanso necesario, mediante la limitación de la jornada laboral y el respeto a las vacaciones de las personas trabajadoras.
> 2. Impulsar la creación de un plan de uso de las tecnologías de la comunicación fuera de la jornada laboral con el objetivo de educar digitalmente tanto al empresariado como a los trabajadores y trabajadoras.
> 3. Impulsar la creación por parte del Instituto Nacional de Estadística de indicadores de medición del estrés laboral de los trabajadores y trabajadoras.
> 4. Impulsar la realización de un estudio que analice si el uso intensivo de las tecnologías de la información y de la comunicación (mensajería y correos electrónicos o dispositivos móviles) puede llegar a provocar problemas de adicción o dependencia."

La proposición no de ley supone un primer paso para adecuar los derechos básicos del trabajador a la sociedad digital y evitar un nuevo modelo de esclavitud laboral. Las propuestas del texto podrían completarse con un código de buenas prácticas entre las empresas y los trabajadores, de manera que, junto con la regulación establecida por convenio colectivo pudiera quedar suficientemente claro el uso de las

[41] La Ley francesa reconoce que en las empresas de más de 50 trabajadores, la dirección y los representantes de los trabajadores deberán llegar a acuerdos para establecer "las modalidades del pleno ejercicio por el trabajador de su derecho a la desconexión y la puesta en marcha por la empresa de dispositivos de regulación de la utilización de dispositivos digitales, a fin de asegurar el respeto del tiempo de descanso, vacaciones, jornada establecida, así como de su vida personal y familiar".

[42] BOCG, Congreso de los Diputados, 17 de marzo, 2017, núm. 125, p. 10. Proposición no de Ley presentada por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú-Podem-En Marea, sobre el derecho a la desconexión laboral fuera del horario de trabajo.

tecnologías fuera del horario laboral, con independencia de la regulación legal del derecho a la desconexión digital.

3. La protección de datos de carácter personal

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 (RGPD), tiene por objeto fijar "las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y las normas sobre la libre circulación de datos en la Unión" (art. 1). El RGPD se ha dicho tiene "alma de Directiva" y contiene varias disposiciones que necesitarán una normativa nacional que los desarrolle. Para completar y desarrollar el RGPD, allí donde remita a la legislación de los Estados miembros, se ha aprobado el Proyecto de Ley Orgánica de Protección de Datos (PLOPD) (noviembre 2017), que sustituirá a la LOPD y será, junto con el RGPD, cuando entre en vigor, la normativa vigente en materia de protección de datos.

El artículo 1.2 del PLOPD dice: "el derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta Ley Orgánica".

El RGPD contiene algunas disposiciones normativas que se dirigen a los Estados miembros para que adopten normas que las completen (por ejemplo, las autoridades de supervisión). Otras disposiciones requieren normas estatales (por ejemplo, el tratamiento de los datos sensibles).

Hay otras que autorizan a los Estados miembros a regular determinadas materias. El ejemplo es el de la edad mínima a partir de la cual los menores pueden otorgar consentimiento para que sus datos sean tratados sin autorización de sus padres o tutores. El RGPD fija esa edad en 16 años, pero permite a los Estados miembros que la reduzcan hasta un límite mínimo de 13.

Algunos de estos desarrollos normativos están incluidos en el PLOPD. Otros se incluirán en otras normas sectoriales.

3.1. Ámbito de aplicación

El RGPD distingue entre ámbito de aplicación material y territorial. Tanto el RGPD (art. 2) como el PLOPD (art. 2) se aplican a todos los tratamientos total o parcialmente automatizados de datos y a los tratamientos no automatizados de datos contenidos o destinados a ser incluidos en un fichero.

Quedan excluidos del ámbito de aplicación del RGPD los siguientes tratamientos (art. 2.2):

- Los realizados en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.
- Los realizados por los Estados miembros cuando lleven a cabo tratamientos relacionados con la Política Exterior y de Seguridad Común de la UE.
- Los efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
- Los realizados por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

El PLOPD regula cómo los herederos de la persona fallecida o las personas que ésta haya designado podrán acceder y disponer tanto sobre sus datos personales como sobre sus contenidos digitales (art. 3, disposición adicional séptima).

Según el artículo 3.1, el RGPD será aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

3.2. Principios

Los principios que el RGPD establece en el artículo 5 son similares a los de la Directiva 95/46, pero presenta algunas novedades.

A. Licitud, transparencia y lealtad

La licitud del tratamiento se relaciona con la necesidad de que esté amparado en una de las bases jurídicas que enumera el artículo 6 del RGPD.

La transparencia se requiere en el momento de recabar los datos (art. 11 PLOPD), en el ejercicio de los derechos (art. 13 PLOPD) y en la publicidad que se impone a las administraciones públicas de incluir en la página web el "inventario de actividades de tratamiento" (art. 31.2 PLOPD).

Asimismo, el RGPD prohíbe que los datos sean tratados de forma desleal para el interesado o sin proporcionarle la información necesaria para que entienda el objeto y fines del tratamiento, sus consecuencias y posibles riesgos, y pueda, en su caso, decidir sobre él (por ejemplo, que se oculte alguna finalidad del tratamiento, o que esa finalidad se exprese de forma vaga y confusa).

B. Limitación de la finalidad

Obliga a que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas. La finalidad del tratamiento ha de estar claramente definida.

Prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines (art. 6.4 RGPD).

C. Minimización de datos

Solo serán tratados los datos "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

D. Exactitud

Los datos deben ser correctos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.

E. Limitación del plazo de conservación

La conservación de los datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, desprovistos de todo elemento que permita identificar a los interesados. Las excepciones están previstas en el artículo 17.3 del RGPD.

F. Integridad y confidencialidad

Estos principios son nuevos en el RGPD y no se mencionaban en la Directiva. Imponen a quienes tratan datos la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

El artículo 5 del PLOPD obliga a la confidencialidad a los responsables, encargados y todas las personas que intervengan en cualquier fase del tratamiento de datos.

G. Responsabilidad proactiva

El artículo 5 del RGPD establece el principio denominado de "responsabilidad proactiva". Este principio se define en el artículo 24 del RGPD: "teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento".

La responsabilidad última atañe al responsable, pues es quien decide que se inicie un tratamiento, su finalidad, los datos que van a ser tratados y cuáles son las actividades

de tratamiento que se van a realizar. Además, se exige que el responsable adopte medidas preventivas dirigidas a reducir los riesgos de incumplimiento.

La responsabilidad proactiva del responsable del tratamiento incluye el autoanálisis, crítico y continuo, y la documentación (trazabilidad) de las distintas decisiones adoptadas en relación con cada tipo de tratamiento para el cumplimiento de las obligaciones impuestas, los accesos permitidos y las medidas de seguridad implantadas.

Las medidas más importantes previstas en el RGPD son:

- Obligación de transparencia del responsable hacia el sujeto de los datos en relación al conjunto de tratamientos realizados y los datos recogidos.
- Obligación de facilitar el ejercicio de los derechos reconocidos a los sujetos de los datos, en particular los derechos de acceso a los datos almacenados por el responsable, rectificación de los datos erróneos y cancelación de los datos no necesarios.
- Obligación de tener un Delegado de Protección de Datos que, además de asesorar y supervisar el cumplimiento de la normativa de protección de datos, canalice la relación con las autoridades de control y con los afectados por el tratamiento.
- Obligación de tener un Registro de actividades de tratamiento, que sustituye a la de la notificación de ficheros a la Autoridad de Control.
- Obligación de publicar el Inventario de actividades de tratamiento en la página web (administraciones públicas).
- Obligación de realizar análisis de riesgos para la seguridad, precisar los requisitos de privacidad desde el diseño y por defecto, y de realizar las evaluaciones de impacto exigidas en el RGPD.
- Obligación de adoptar las medidas de seguridad apropiadas tras el análisis de riesgo, lo que implica el mantenimiento de las mismas y la definición de un ciclo de vida de los datos y de las medidas.
- Obligación de notificar las brechas de seguridad tanto a las autoridades de control como a los sujetos de los datos que han podido ser comprometidos.

Especial mención requieren los principios de protección de datos desde el diseño y protección de datos por defecto, contemplados en los considerandos 78 y 108 y en el artículo 25 del RGPD.

El principio de protección de datos desde el diseño ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar los desarrollos. Las medidas han de informar toda su estructura. La obligación de que se adopten los principios de privacidad desde el diseño recae en el responsable del tratamiento.

La selección de las medidas será resultado de un análisis de riesgos en relación a la probabilidad y gravedad de que afecten a los derechos y libertades de las personas físicas y se aplicarán teniendo en cuenta el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento.

El concepto de privacidad por defecto está en el artículo 25.2 del RGPD y consiste en limitar el tratamiento a los datos personales que sean estrictamente necesarios para cada uno de los fines descritos, independientemente del conjunto de datos recogidos.

3.3. La legitimación para el tratamiento de datos personales

El RGPD enumera en su artículo 6.1 las bases jurídicas que legitiman el tratamiento de datos personales en términos de igualdad:

> "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
>
> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
>
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
>
> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

> f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

A continuación se analiza cada una de estas bases:

A. El consentimiento

El RGPD define el consentimiento como una manifestación de voluntad libre, específica, informada e inequívoca (art.7), por la que el afectado acepta el tratamiento mediante una declaración o una clara acción afirmativa (art. 6 PLOPD).

El considerando 32 del RGPD precisa qué se entiende por prestación válida del consentimiento:

- Se considera que puede existir un acto afirmativo claro en supuestos como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.
- También puede considerarse un acto afirmativo marcar una casilla de un sitio web en Internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.
- El silencio, las casillas premarcadas o la inacción del afectado no constituyen un consentimiento válido.
- En el caso de que el tratamiento tenga varios fines deberá prestarse para cada uno de ellos. No obstante, sería posible agrupar varias finalidades en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros), si bien deberían desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo, tratamiento por quien recaba los datos y cesión a terceros).

El considerando 42 señala que “el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno”.

El considerando 43 dice: “Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”. Además, presume que “el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento”.

Los consentimientos obtenidos con anterioridad a la aplicación efectiva del RGPD, el 25 de mayo de 2018, únicamente mantendrán su validez si se ajustan a las previsiones del Reglamento que, como se ha señalado, exige una declaración positiva o una clara acción afirmativa (considerando 171).

Esta previsión se recoge en la de la Disposición transitoria sexta del PLOPD: “cuando el tratamiento se basa en un consentimiento otorgado con anterioridad a la aplicación del RGPD, no será necesario recabar nuevamente dicho consentimiento si la forma en que se otorgó se ajusta a las condiciones del RGPD”.

El consentimiento es revocable debiendo informarse al afectado de esta posibilidad. La revocación del consentimiento debe poder realizarse por procedimientos tan sencillos como los utilizados para obtenerlo, pero no tiene efectos retroactivos, no afectando a la licitud de los tratamientos realizados hasta ese momento.

B. La relación contractual

El RGPD establece en su artículo 6.1.b que será lícito el tratamiento "necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales".

C. Tratamientos necesarios para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

La base jurídica del tratamiento de datos personales por parte de las administraciones públicas será, como regla general, la contemplada en el artículo 6.1 (apartados c, e) del RGPD.

Respecto de estas bases jurídicas el RGPD y el artículo 8 del PLOPD prevén que solo será legítimo el tratamiento si así lo establecen una norma de Derecho de la Unión o una ley (directamente, si se trata del cumplimiento de una obligación legal o a través de una atribución de competencias si se trata del ejercicio de poderes públicos).

El RGPD y el artículo 8.1 del PLOPD añaden que:

- la finalidad del tratamiento para el cumplimiento de una obligación legal debe quedar determinada en la norma que la establezca y
- la finalidad del tratamiento para el cumplimiento de una misión de interés público o para el ejercicio de poderes debe ser necesaria y proporcional para el cumplimiento o ejercicio de los mismos.

El considerando 45 del RGPD señala que una misma norma puede ser suficiente como base para varias operaciones de tratamiento.

D. El interés vital

El tratamiento de datos personales es lícito cuando sea necesario para proteger intereses vitales del interesado o de otra persona física (art. 6.1.d RGPD).

El considerando 46 del RGPD atribuye a esta base jurídica para el tratamiento un carácter subsidiario al indicar que la misma únicamente debe aplicarse cuando el

tratamiento no puede basarse en otra base jurídica distinta (cita como ejemplos el tratamiento con fines humanitarios, incluido el control de epidemias y su propagación o las situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano).

E. El interés legítimo

El RGPD incluye el interés legítimo del responsable o de un tercero como base jurídica para el tratamiento de datos personales (art.6.1.f RGPD).

Sin embargo, no basta con la concurrencia de un interés legítimo sino que es necesario que prevalezca sobre los intereses, derechos o libertades fundamentales del interesado.

Por tanto, será necesario realizar en cada caso concreto una ponderación para poder determinar la prevalencia o no del interés legítimo. El RGPD exige que esa ponderación sea especialmente cualificada cuando el afectado sea un menor.

El Reglamento advierte que el interés legítimo no puede ser una base jurídica aplicable a los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones, al señalar que es el propio legislador el que debe establecer por ley la base jurídica para el tratamiento de datos por parte de las autoridades públicas.

El RGPD refuerza algunas de las garantías para el tratamiento de datos personales cuando su base jurídica sea el interés legítimo. Así, en relación con el deber de informar al interesado sobre el tratamiento de los datos, exige que se especifiquen los intereses legítimos concretos del responsable o del tercero que lo realizarán, tanto si los datos se han obtenido del afectado como si los han obtenido de otra fuente (arts. 13.1.d y 14.2.b del RGPD).

El RGPD también refuerza el derecho a oponerse en cualquier momento al tratamiento de datos personales por motivos relacionados con su situación personal cuando su base jurídica sea el interés legítimo, estableciendo que el responsable dejará de tratar los datos personales salvo que acredite “motivos legítimos

imperiosos" que prevalezcan sobre los intereses, derechos y libertades del afectado (art. 21.1).

Los considerandos 47 a 49 recogen algunas aclaraciones sobre esta base jurídica.

Los citados considerandos recogen algunos ejemplos de intereses legítimos, aunque sin considerarlos por sí mismos como prevalentes:

- La prevención del fraude, siempre que se cumpla el principio de minimización (considerando 47);
- El marketing directo (considerando 47);
- Las transmisiones de datos en grupos de empresas para fines administrativos internos como puede ser la centralización de datos de clientes o empleados (considerando 48);
- Las transmisiones de datos para garantizar la seguridad de las redes (por ejemplo a los equipos de respuesta a emergencias informáticas –CERT– o de respuesta a incidentes de seguridad informática –CSIRT–), para impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de "denegación de servicio" y daños a los sistemas informáticos y de comunicaciones electrónicas (considerando 49).

3.4. Tratamiento de categorías especiales de datos (datos especialmente protegidos)

El RGPD incluye en el concepto de "categorías especiales de datos" los hasta ahora denominados "datos especialmente protegidos" por la LOPD: las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona. Incorpora además dos nuevas categorías de datos como son los datos genéticos (datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos, en particular, del análisis de una muestra biológica) y los datos biométricos (datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o

conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos).

La regla general contemplada en el RGPD es la prohibición del tratamiento de categorías especiales de datos (art. 9).

No obstante, se recoge un amplio abanico de excepciones a esta regla general:

> "a) El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
> b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
> c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
> d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
> e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
> f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
> g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
> h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social".

Sobre los tratamientos realizados con las finalidades citadas se prevé que el tratamiento se realice por un profesional sujeto a deber de secreto o bajo su responsabilidad, así como por cualquier otra persona sujeta a la obligación de secreto, siempre que se realice de acuerdo con el Derecho de la UE o de los Estados miembros.

> "i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios;
> j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (…)".

El artículo 9.4 del RGPD admite que los Estados miembros puedan mantener o introducir condiciones adicionales, incluidas limitaciones, sobre los tratamientos de datos genéticos, biométricos o de salud.

El artículo 9 del PLOPD hace algunas precisiones en relación con las categorías especiales de datos:

- Partiendo de la posibilidad admitida por el RGPD de que el derecho de los Estados miembros puedan establecer que el consentimiento del afectado no permita excepcionar la prohibición de tratar datos sensibles, el PLOPD establece que "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico", si bien a continuación precisa que dichos datos podrán tratarse al amparo de los restantes supuestos contemplados en el artículo 9.2 del RGPD, cuando así proceda.
- Para determinados tratamientos (los contemplados en las letras g, h, i del artículo 9.2 del RGPD), exige que estén amparados en una norma con rango de ley si están fundados en el Derecho español, ley que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
- Incluye una referencia específica sobre el tratamiento de datos de salud estableciendo que "la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de

asistencia sanitaria y social, pública y privada y de los seguros de asistencia sanitaria".

En relación con el tratamiento de datos de condenas, medidas de seguridad e infracciones penales, el RGPD prevé algunas especialidades. Estas categorías de datos sólo podrán tratarse bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas (art. 10 RGPD). A este respecto, el PLOPD reconoce la competencia exclusiva del Ministerio de Justicia para la llevanza de un registro que recoja la totalidad de los datos relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas (art. 10.2).

Por último, la vigente LOPD establece un régimen reforzado de protección para los datos relativos a las infracciones y sanciones administrativas al calificarlas como datos especialmente protegidos. El RGPD no contempla una previsión similar. El PLOPD, en aplicación del principio de minimización de datos regulado en el artículo 5.1.c del RGPD, establece que el tratamiento de este tipo de datos sea realizados por los órganos competentes para la declaración de infracciones y la imposición de sanciones, limitándose su tratamiento a los estrictamente necesarios para la finalidad perseguida.

3.5. Derecho de información en la recogida de datos

El RGPD incrementa la información que habrá de facilitarse al interesado (capítulo III –derechos del interesado-).

En sus artículos 12 y 13, el RGPD desarrolla ampliamente la "Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado" (art. 12), y la "Información que deberá facilitarse cuando los datos personales se obtengan del interesado" (art. 13).

El responsable del tratamiento deberá informar sobre los siguientes aspectos:

- Identidad y datos de contacto del responsable y, en su caso, de su representante.
- Datos de contacto del delegado de protección de datos.
- Fines y base jurídica del tratamiento.
- Intereses legítimos del responsable o de un tercero.
- Destinatarios o categorías de destinatarios de los datos personales.
- Transferencias internacionales previstas.
- Plazo de conservación.
- Derechos de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad.
- Posibilidad de revocación del consentimiento.
- Derecho a presentar una reclamación ante una autoridad de control.
- En el supuesto de que la comunicación de datos personales sea obligatoria, se deberá informar de las posibles consecuencias de no facilitar los datos.
- Información sobre la posible existencia de decisiones automatizas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias previstas.

El artículo 14 del RGPD establece una regulación más exigente en relación con la "Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado".

Dicho precepto dice que, si los datos no se recaban del interesado, deberá, además, informársele de las "Categorías de datos que se van a tratar", de la "Fuente de la que proceden los datos personales", y, en su caso, sobre si proceden de "Fuentes de acceso público".

Asimismo, en el RGPD prescribe el plazo aplicable para informar al interesado en caso de no recabarse los datos directamente del mismo, siendo este –con carácter general- de un mes.

El RGPD establece excepciones específicas al deber de información, recogidas en sus artículos 13.4 y 14.5, de forma que no se aplicará lo anteriormente expuesto:

- Cuando el interesado ya disponga de la información.
- En los supuestos de esfuerzo desproporcionado, en caso de tratamiento con fines de archivo, estadísticos o de investigación científica o histórica.
- En los supuestos de existencia de una previsión legal expresa de tratamiento o revelación, con medidas oportunas de protección.
- En los supuestos de existencia de una obligación de secreto legal o profesional.

3.6. Ejercicio de derechos relativos a la protección de datos

Como titular de sus datos de carácter personal, el afectado por el tratamiento puede ejercitar ante el responsable que esté tratando dichos datos personales, los derechos de acceso, de rectificación, de supresión -incluida su variante de derecho al olvido-, de portabilidad, de oposición, y de limitación del tratamiento.

El considerando 59 del RGPD, anticipa las líneas generales de la protección al señalar que "deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento estará obligado a responder a las solicitudes del interesado sin dilaciones indebida y, a más tardar, en el plazo de un mes, así como a explicar sus motivos en caso de denegación."

Los referidos derechos se regulan en los artículos 15 a 22 del RGPD.

El artículo 12 del PLOPD, bajo el título de "Disposiciones generales sobre ejercicio de los derechos", señala:

> "1.□ Los derechos reconocidos en los artículos 15 a 22 del RGPD podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá atender, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del RGPD, se estará a lo dispuesto en aquellas."

A. Derecho de acceso

A través del ejercicio de este derecho, los interesados por los tratamientos pueden conocer si sus datos de carácter personal están siendo tratados por parte del responsable del tratamiento, qué datos son objeto de dicho tratamiento, la finalidad del mismo, el origen de los citados datos y si se han comunicado o se van a comunicar a un tercero.

A su vez, en la aplicación del RGPD (art. 15 "Derecho de acceso del interesado") se amplía la posibilidad de conocimiento:

"1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del

tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros."

El artículo 13 del PLOPD precisa las condiciones para el ejercicio de este derecho en algunos supuestos:

- Cuando el responsable trate una gran cantidad de información relativa al interesado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitar, antes de facilitar la información, que especifique los datos o actividades de tratamiento a los que se refiere su solicitud (párr. 2 del art. 13.1).
- El derecho de acceso se entenderá otorgado si la Administración u Órgano responsable del tratamiento facilita al interesado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad (art. 13.2).
- Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello (art. 13.3).

El RGPD establece la gratuidad del primer acceso mediante copia de la información, posibilitando la exigencia de un canon orientado a sufragar los costes de las ulteriores solicitudes.

El derecho de acceso es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. También es independiente del derecho de acceso a la documentación en un procedimiento administrativo, regulado por la normativa sobre régimen jurídico y procedimiento administrativo común.

Por su parte, el acceso a la historia clínica se regula específicamente en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP), si bien la autoridad competente en materia de protección de datos podrá tutelar este acceso en caso de que -una vez ejercitado- la respuesta no sea satisfactoria para el ciudadano, o no se haya respondido en los plazos previstos.

Además, esta Ley permite el acceso a la historia clínica de los pacientes fallecidos a personas vinculadas con él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

B. Derecho de rectificación

De acuerdo con el artículo 16 del RGPD, mediante su ejercicio ante el responsable del tratamiento, el titular de los datos personales tiene derecho a obtener sin dilaciones indebidas la modificación de sus datos personales inexactos o incompletos, debiendo en la solicitud de rectificación indicar qué datos desea que se modifiquen o corrijan. A dicha solicitud, el titular de los datos -solicitante de la rectificación-, deberá acompañar la documentación justificativa en la que base su pretensión (art. 14 PLOPD).

C. Derecho de supresión y derecho al olvido

El derecho al olvido está reconocido en el artículo 17 del RGPD[43]. El derecho al olvido recoge la doctrina sentada por la Sentencia de 13 de mayo de 2014 del TJUE[44], en la que establecía que el uso de datos que realizan los motores de búsqueda es un tratamiento de datos, y por tanto está sometido a las normas correspondientes. La sentencia reconoce a los sujetos el derecho a solicitar, en determinadas condiciones, que los enlaces a los datos personales del interesado no aparezcan cuando se realice una búsqueda con su nombre en Internet.

El derecho al olvido en Internet pretende evitar la difusión de información de un sujeto cuando dicha información no se ajuste a los principios de la protección de datos, por ejemplo, a los principios de pertinencia, adecuación, finalidad, o no tenga interés general, etc. El derecho al olvido es la versión digital de los derechos de cancelación y de oposición que podían ejercerse respecto de un tratamiento de datos. Hay que recordar que este derecho forma parte del contenido esencial del derecho a la protección de datos, por ser un instrumento que permite mantener el control sobre los datos de carácter personal en el entorno digital, y supera las carencias que el ejercicio del derecho de rectificación y cancelación habían demostrado para los buscadores de información.

El considerando 66 del RGPD habla del derecho al olvido en el entorno en línea, reconociendo que el derecho de supresión, "debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para

[43] Sobre el derecho al olvido vid., Mieres Mieres, L. J., *El derecho al olvido digital*, Fundación Alternativas, disponible en: http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf; y Hernández Ramos, M., *Cuaderno Red de Cátedras Telefónica. El derecho al olvido digital en la Web 2.0*, 2013, Salamanca.

[44] STJUE de 13 de mayo de 2014, caso Mario Costeja/AEPD v. Google (C-131/12). La sentencia reconoce el derecho a la desindexación de enlaces en motores de búsqueda, bajo determinadas circunstancias. Esta sentencia viene precedida de la de abril de 2014 en el caso *Digital Rights Ireland*, en la que el TJUE anuló la Directiva 200624/CE, de retención de datos por considerarla contraria a la privacidad.

informar de la solicitud del interesado a los responsables que estén tratando los datos personales."

Por su parte, el considerando 65 destaca especialmente la situación de la publicación en Internet de los datos siendo niño, sin ser plenamente consciente de los peligros de dicho acto y reconociendo el deseo de querer suprimir, ya en la edad adulta, sus datos personales. El mismo considerando establece **limitaciones al derecho al olvido** cuando haya de protegerse la libertad de información o la libertad de expresión, para cumplir una obligación legal, para cumplir una misión realizada en interés público, o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos o para la formulación, el ejercicio o la defensa de las reclamaciones (art. 17.3 RGPD).

El derecho al olvido está recogido en el artículo 17 del RGPD como el derecho "a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes (…)", circunstancias que enumera el precepto y que hacen referencia a la quiebra del principio de finalidad, a la retirada del consentimiento en que se basa el tratamiento, a la oposición del tratamiento de datos de acuerdo con lo previsto en el Reglamento, al tratamiento ilícito de los datos personales, a la supresión de los datos para cumplir una obligación legal y si los datos se han obtenido en relación con la oferta de servicios de la sociedad de la información dirigida al menor si es mayor de 16 años o menor, pero si el consentimiento lo dio el titular de la patria potestad o tutela del niño.

El artículo señala en el apartado 2 que: "Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los

datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos."

¿Qué reconoce el derecho al olvido? El derecho al olvido reconoce el derecho del sujeto a que sus datos personales no se difundan de manera ilimitada y sin control a través de Internet, por medio de los buscadores de información, cuando, como tratamiento de datos que realizan dichos buscadores, dicho tratamiento no se ajusta a lo establecido en la normativa vigente. En Internet, el motor de búsqueda de información difunde una información sobre un sujeto que ha sido colgada por el editor, y la difunde de forma universal. El buscador accede a un conjunto de enlaces previamente indexados y ofrece al usuario una relación de direcciones web que le remiten a páginas en las que aparecen las palabras seleccionadas por el usuario. Por lo que, a la información buscada por el usuario, se añade la que el propio buscador facilita sobre la misma persona, lo que ofrece una información amplia sobre cuestiones relacionadas con el sujeto en el ámbito de la protección de datos y que puede provocar una lesión en este derecho. En palabras de la STJUE "la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido del artículo 2 de la Directiva 95/46, de 24 de octubre de 1995 (…)" (fto. jco. 1). La difusión de esta gran cantidad de información se realiza sin que previamente se haya comprobado su actualización, o su veracidad, o la pertinencia y adecuación a la finalidad perseguida por la persona que busca la información a través de los buscadores. No solo puede resultar un problema la falta de veracidad de los datos, sino que la finalidad con la que los datos fueron recogidos y tratados en su inicio puede haber desaparecido, circunstancia que convierte el tratamiento de datos en ilícito. La STJUE resaltaba la importancia del factor tiempo en Internet, ya que el tratamiento de datos debe cumplir con los requisitos de calidad del artículo 4 de la LOPD durante todas las fases del tratamiento, esto es, no solo en su recogida sino también en todo momento posterior. Un tratamiento que en su momento inicial fue adecuado y pertinente puede devenir con el transcurso del tiempo en inadecuado y apartarse de la finalidad que justificó la recogida y el tratamiento de datos. En este

caso, el daño que se produce en el honor y la intimidad de la persona puede ser desproporcionado en relación con el derecho que ampara el tratamiento de datos. Al igual que, la recepción masiva de información, que no se realiza al amparo de ningún interés general, puede provocar una invasión en nuestra intimidad y lesionar el derecho a la protección de datos.

El ejercicio del derecho al olvido por parte del sujeto obliga a suprimir la información del buscador, pues la STJUE considera responsable del tratamiento al gestor de un motor de búsqueda. En otras palabras, obliga al responsable a retirar el enlace que lleva a la información personal, es decir, a dejar de indexar dichos contenidos, con independencia de que la publicación en dichas páginas sea en sí mismo lícita. Sin embargo, el derecho al olvido no obliga a eliminar la información de las fuentes originarias, por lo que dicha información puede seguir apareciendo a través de cualquier otro término que no sea el nombre del sujeto que ejerció su derecho al olvido. Por tanto, la información no se puede borrar de Internet ejercitando el derecho al olvido, pues podría vulnerarse el derecho a la información, pero se dificulta su búsqueda a través de los buscadores. Es decir, a través de derecho al olvido se reclama la cancelación de los datos, pero no de la página web del medio de comunicación que transmite la información, sino la adopción de medidas tecnológicas necesarias para que la página web de la noticia no sea indexada por los motores de búsqueda en Internet. La publicación de la noticia en los medios de prensa digitales es constitucional, es fruto del ejercicio del derecho de información. Ahora bien, una vez publicada en aras del interés general y actual de lo noticiado, el tratamiento de datos de carácter personal que se produce cuando se vincula la información que transmite la noticia a través de los motores de búsqueda de Internet, utilizando como palabras clave los datos personales (básicamente nombre, apellido, profesión, etc.) nos remite de nuevo a la información originaria. Debido al paso del tiempo, el interés de la misma puede ir decayendo, si la persona carece de relevancia pública y los hechos con los que aparecen relacionados no presentan interés histórico. Por ello, aunque en un principio el tratamiento de esos datos se ajustaba a la ley, con el tiempo, ha devenido en inadecuado, no pertinente, desproporcionado y desligado de la finalidad que justificó su tratamiento. Por tanto, de acuerdo con la legislación de protección de datos hay que eliminarla.

El **derecho al olvido no es absoluto**, tal y como reconoce la STJUE (fto. jco. 4), sino que admite limitaciones, en especial, el derecho a la información. De hecho el RGPD recoge el derecho a la información como límite frente al derecho al olvido (art. 17.3.a RGPD). Desde luego el derecho al olvido prevalece frente al interés económico del gestor del motor de búsqueda, pero también sobre el interés del público en acceder a la información del sujeto en una búsqueda basada en el nombre de la persona. En cambio, el derecho al olvido no prevalecería, a tenor de la STJUE, por razones concretas, como el papel desempeñado por el interesado en la vida pública, pues en este caso, la injerencia en sus derechos fundamentales se justifica por el interés del público en acceder a la información de que se trate. Llama la atención aquí que el TJUE no realice una mayor precisión pues, aunque el derecho a la intimidad del sujeto que ejerce una actividad pública pueda quedar limitado, no desaparece absolutamente y ha de quedar un ámbito mínimo protegido por el derecho, vedado al conocimiento del público. En realidad la protección de la información en la fuente originaria deriva del ejercicio del derecho a la información, del derecho a "recibir libremente información veraz por cualquier medio de difusión". Este derecho, esencial en un Estado democrático prevalece frente a otros derechos constitucionales, debido a la posición preferente que le ha reconocido el TC siempre y cuando los hechos comunicados sean de relevancia pública y veraces (por todas STC 107/1988 y STC 240/1992). Entre las razones que los tribunales valoran para realizar un juicio de proporcionalidad entre el derecho a la información y el derecho al olvido podemos señalar la antigüedad de los datos publicados, la ausencia de circunstancias personales del afectado que determinen una especial relevancia de interés público en mantener dicha información, el daño en la reputación profesional que el afectado puede sufrir, etc., precisando algo más la doctrina del TJUE.

El derecho al olvido se ejerce ante la entidad que está tratando los datos de carácter personal. En el caso del derecho al olvido en Internet se ejercería ante los buscadores (Google, Yahoo, Terra). Estos buscadores, tras la STJUE y diferentes decisiones judiciales, han habilitado formularios y procedimientos para solicitar la retirada de la información a través del ejercicio del derecho. Una vez ejercitado el derecho puede ocurrir que el buscador atienda la solicitud del sujeto, lo que originará la indexación de la información del sujeto. Puede ocurrir, por el contrario, que el buscador ignore la

petición del individuo. Ante la inactividad del buscador o la respuesta insatisfactoria, el sujeto puede dirigirse a la AEPD para solicitar su tutela, en virtud del artículo 18.1 de la LOPD. La decisión de la AEPD es recurrible ante los tribunales de justicia.

D. El derecho a la portabilidad de los datos

El artículo 20 del RGPD regula el **derecho del sujeto a la portabilidad de los datos** como:

> "el derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otros responsable sin que lo impida el responsable al que se los hubiera facilitado, cuando:
> a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
> b) el tratamiento se efectúe por medios automatizados."

El derecho a la portabilidad es el **derecho del sujeto a "llevarse"** los datos entregados de forma voluntaria, así como **"entregarlos"** a otro responsable, de recibir y transmitir habla la norma. Se trata de dos acciones que no tienen por qué producirse sucesivamente. En primer lugar, el derecho a la portabilidad reconoce el derecho a recibir los datos de carácter personal en un formato estructurado, de uso común y legible por máquina, para después almacenarlos para uso personal, y poder posteriormente reutilizarlos, sin transmitirlos a otro responsable. Este aspecto del derecho a la portabilidad es un complemento del derecho de acceso. En segundo lugar, el derecho a la portabilidad contempla el derecho a transmitir los datos personales de un responsable de tratamiento a otro responsable de tratamiento, sin ningún tipo de obstáculo por ninguna de las partes. Se evita de esta manera la retención de los datos por parte de un responsable y se facilita el "empoderamiento" de los datos por parte del usuario, lo que permite y refuerza el control de los datos del sujeto, que puede decidir el intercambio de sus datos y su reutilización posterior. El derecho a la portabilidad de los datos ha sido analizado e interpretado en el Documento elaborado por el Grupo de Trabajo del artículo 29 (GT29)[45]. El Documento ha señalado los aspectos interpretativos a tener encuentra para un correcto ejercicio del derecho a la portabilidad y una respuesta adecuada por parte de

[45] Directrices sobre el derecho a la portabilidad de datos, adoptado el 13 de diciembre de 2016. Disponible en http://ec.europa.eu/justice/data-protection/index_en.htm

los responsables del tratamiento que han de entregar los datos cumpliendo las condiciones del artículo 20 del RGPD.

Los **supuestos** en los que cabe ejercitar el derecho a la portabilidad contemplan las siguientes circunstancias: cuando el sujeto haya consentido el tratamiento de los datos para uno o varios fines específicos, o cuando el interesado consintió el tratamiento de categorías de datos especiales para uno o más fines específicos, salvo que el Derecho de la Unión o de los Estados miembros determine la prohibición de tratar categorías especiales de datos incluso con el consentimiento del sujeto, o bien cuando el tratamiento de datos es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a este de medidas precontractuales. En todos estos casos, el artículo 20 del RGPD exige que los datos sean tratados de forma automatizada. Por tanto, el derecho a la portabilidad no se puede ejercitar cuando el tratamiento de datos no está basado en el consentimiento o en un contrato, y tampoco en tratamiento de datos en soporte papel.

El derecho a la portabilidad debe cubrir, además de los datos facilitados por el sujeto de forma voluntaria, también los datos de los interesados que se generan y recaban a partir de la actividad de los mismos, pero no aquellos otros datos que se han generado como consecuencia del tratamiento realizado por el responsable. Sin la inclusión de todos los datos que corresponde, el ejercicio del derecho a la portabilidad quedaría incompleto y podría iniciarse el procedimiento de reclamación previsto, ante la falta de satisfacción del derecho a la protección de datos. Solamente se entregarán los datos personales del sujeto, no aquellos otros que puedan contener información de otros individuos. Entre los datos que pueden entenderse proporcionados por el usuario, según el GT29, podemos incluir los datos entregados de forma consciente y activa por el sujeto y los datos entregados como consecuencia del uso del servicio o dispositivo, por ejemplo, el historial de búsqueda o los datos de ubicación de una persona. Sin embargo, no serían objeto del derecho a la portabilidad los datos "inferidos" o "deducidos", teniendo como base los datos proporcionados por el interesado. En este sentido, el responsable del tratamiento puede haber desarrollado un perfil del usuario, que no se considera en sentido estricto "datos proporcionados" por el interesado y que sin embargo sobre ellos se puede ejercitar el derecho de

acceso (art. 15 RGPD) y el derecho a no ser objeto de una decisión basada en la elaboración de un perfil (art. 22 RGPD).

Los datos han de trasmitirse de manera estructurada, de uso común y de lectura mecánica, es decir, con características que apuntan, tanto a las condiciones en las que han de entregarse como al medio, y con un formato que permita la interoperabilidad, que es el resultado que se quiere alcanzar. El considerando 68 del RGPD aclara el significado de la expresión interoperable. El término interoperable se define en la UE como "la capacidad de que organizaciones dispares y diversas actúen en pos de objetivos comunes mutuamente beneficiosos y acordado en relación con la puesta en común de información y conocimiento entre las organizaciones a través de los procesos empresariales que respaldan, mediante el intercambio de datos entre sus sistemas de TIC respectivos"[46]. Por lo que respecta a la idea de lectura mecánica, el considerando 21 de la Directiva 2013/37/UE[47], define legible por máquina como "un formato de archivos estructurado de forma que las aplicaciones informáticas puedan fácilmente identificar, reconocer y extraer datos específicos, inclusive exposiciones personales de hechos, y su estructura interna. Los datos codificados en archivos que están estructurados en un formato legible por maquina son datos legibles por máquina. Los formatos legibles por máquina pueden ser de uso libre o patentados; pueden ser estándares forales o no. Los documentos codificados en un formato de archivos que limita el tratamiento automático, debido a que sus datos no pueden extraerse o no pueden extraerse fácilmente, no deben considerarse que tienen un formato legible por máquina. Los Estado miembros deben alentar cuando proceda la utilización de formatos de uso libre y legibles por máquina".

Por tanto, los formatos en los que se proporcionen los datos deben ser interoperables y el GT29 recomienda que los sectores implicados trabajen conjuntamente para dotarse de una serie de normas comunes y formatos interoperables para asegurar el ejercicio del derecho a la portabilidad de los datos. El Marco de la Interoperabilidad

[46] Definición contenida en el art. 2 de la Directiva núm. 922/2009/CE, del Parlamento Europeo y del Consejo de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (ISA) OJ L 260, 3.10.2009, p. 20

[47] Directiva que modifica la Directiva 2003/98/CE, relativa a la reutilización de la información del sector público.

Europeo ha trabajado para crear un escenario común para las organizaciones que presten servicios públicos conjuntamente.

El **ejercicio del derecho a la portabilidad de los datos** ampara la transmisión directa de los datos del interesado de responsable a responsable, siempre que técnicamente sea posible. La portabilidad de los datos, señala el artículo 21.3 del RGPD, no impide el ejercicio del derecho de supresión, salvo que el tratamiento sea necesario para "el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento", siempre que, de acuerdo con el artículo 17, pueda ejercitarse la supresión de los datos. Podrá solicitarse la supresión de los datos en el caso de tratamiento consentido de los datos para uno o varios fines específicos, o en el caso del consentimiento de tratamiento de categorías especiales de datos, o bien en el caso de que lo datos no fueran necesarios en relación con los fines para los que fueros recogidos o tratados. El ejercicio del derecho a la portabilidad no afecta al tiempo de retención original aplicable a los datos respecto de los que ahora se solicita su portabilidad.

El artículo 20.4 del RGPD contiene un **límite general al derecho a la portabilidad** referido al respeto a los derechos y libertades de otros. En este sentido, el considerando 68 del RGPD señala que, "Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento". Para proteger de mejor manera los datos de los terceros cuando se ejercita el derecho a la portabilidad, los responsables del tratamiento, tanto el responsable remitente como el responsable receptor, deberían poner en práctica herramientas que permitan a los interesado seleccionar los datos relevantes y excluir (donde proceda) aquellos que no lo son, porque pertenecen a otros sujetos, tal y como indica el GT29. Ahora bien, al igual que ocurría en el ejercicio del derecho de acceso del artículo 15 del RGPD, "los secretos comerciales o la propiedad intelectual, y en particular, los derechos de propiedad intelectual que protegen programas informáticos", tal y como señala el considerando 63 para el derecho de acceso, no pueden justificar una negativa automática a la solicitud del ejercicio del derecho a la portabilidad de los datos. Los responsables de los

tratamientos deben transmitir los datos del sujeto que solicita la portabilidad de los datos sin desvelar la información cubierta por el secreto comercial o los derechos de propiedad intelectual.

En relación con **el tiempo para atender una solicitud de portabilidad**, el artículo 12.2 del RGPD habla de un plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse por dos meses más en caso necesario, atendiendo a la complejidad y el número de solicitudes. El responsable ha de informar al interesado de dichas prórrogas, en el plazo de un mes desde la recepción de la solicitud. Según el artículo 12.4 del RGPD, si el responsable del tratamiento no da curso a la solicitud de portabilidad, informará al interesado sin dilación, y en el plazo máximo de un mes desde la recepción de su solicitud, le comunicará las razones de su no actuación y la posibilidad de presentar una reclamación ante la autoridad del control, que en este caso es la AEPD, así como ejercitar las acciones judiciales pertinentes. Lo que no podrá hacer nunca el responsable del tratamiento es responder con el silencio a una solicitud de portabilidad. El GT29 recomienda (p.12) establecer un plazo de tiempo en el que debe darse respuesta al interesado y comunicárselo, con el fin de satisfacer las expectativas de los sujetos.

El derecho a la portabilidad **obliga también a los responsables de los tratamientos**. La primera obligación de los responsables del tratamiento a informar, de forma clara y precisa, acerca de la existencia de un nuevo derecho denominado derecho a la portabilidad, de su significado y de cómo se puede ejercitar. Por otro lado, el responsable debe atender debidamente las solicitudes de portabilidad, para lo que puede instalar los medios técnicos necesarios para ello y ofrecer posibilidades para el ejercicio del derecho a la portabilidad. De “herramientas de descarga e interfaces” habla el GT29, como por ejemplo la descarga directa o la transmisión directa de los datos a otro interesado por medio de una API. La API se refiere a “interfaces de aplicaciones o servicios web que ponen a disposición de los responsables del tratamiento para que otros sistemas o aplicaciones puedan enlazarse y trabajar con sus sistemas”, según el GT29. El derecho a la portabilidad, a juicio del documento, “reequilibra” la relación entre los responsables del tratamiento y los interesados al aportarles a estos últimos otro instrumento jurídico de control de sus informaciones

personales y por tanto de su propia vida. El responsable del tratamiento quedarían exonerados de responsabilidad cuando el tratamiento empiece a ser gestionado por el sujeto o por cualquier otra empresa a la que se hayan traspasados los datos. Por otro lado, el responsable del tratamiento receptor de los datos ha de garantizar que los datos sean adecuados y pertinentes en relación con la finalidad del nuevo tratamiento, no debiendo almacenar los datos que no cumplan los requisitos de calidad de los datos del artículo 4 de la LOPD. Los datos que no sean necesarios para cumplir la finalidad del nuevo tratamiento deben ser suprimidos. El responsable que ha recibido los datos se convierte en nuevo responsable del tratamiento y responde del cumplimiento de las garantías previstas en la ley.

Una de las dificultades con que se puede encontrar el responsable del tratamiento es la **identificación del sujeto**. El RGPD no recoge ningún procedimiento para autenticar al interesado, por lo que en principio solicitada la portabilidad de los datos, y según el artículo 12.2 del RGPD, el responsable no puede negarse a facilitar el ejercicio de los derechos, salvo "que pueda demostrar que no está en condiciones de identificar al interesado". En este caso, el interesado puede aportar más información adicional que permita su identificación (art. 11.2 RGPD) y el responsable está facultado para solicitarla (art. 12.6 RGPD). Cuando la información y los datos del sujeto se relacionen con un seudónimo, los responsables de los tratamientos podrán implementar medidas que permitan al sujeto realizar una solicitud de portabilidad y recibir los datos, procediendo a la autenticación del sujeto que ejerce su derecho a la portabilidad.

El derecho a la portabilidad de los datos es un aspecto más de la protección de datos de carácter personal y faculta al interesado para una mayor disposición y control sobre sus datos de carácter personal. En este sentido entendemos que forma parte del contenido esencial del derecho a la protección de datos, por lo que no atender el derecho a la portabilidad, o satisfacerlo de forma incompleta constituye una lesión en el derecho a la protección de datos de carácter personal. Como ha señalado el GT29[48], el derecho a la portabilidad es un instrumento que facilitará la libre

[48] Directrices sobre el derecho a la portabilidad de datos, adoptado el 13 de diciembre de 2016. Disponible en http://ec.europa.eu/justice/data-protection/index_en.htm

circulación de datos personales en la UE y fomentará el mercado único digital. El derecho a la portabilidad busca facilitar el traspaso de datos de un proveedor de servicios a otro, siendo también un instrumento que mejora la competencia al simplificar el cambio de proveedores entre los usuarios.

E. Derecho a la limitación del tratamiento

El RGPD reconoce en su artículo 18 este nuevo derecho –a la "limitación del tratamiento"-, que puede ejercerse cuando se cumpla alguno de los requisitos siguientes:

> "a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
> b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
> c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
> d) el interesado se haya opuesto al tratamiento en virtud del artículo 21.1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado."

El apartado 2 del propio artículo 18 señala: "cuando el tratamiento de datos personales se haya 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 la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro."

Finalmente, de acuerdo con su apartado 3, "todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación."

El artículo 16 del Proyecto de LOPD plasma también el reconocimiento de este derecho por vía de remisión al RGPD. A su vez, dispone que el hecho de que el tratamiento de los datos personales esté limitado deberá constar claramente en el sistema del responsable.

F. El derecho a la protección de la huella digital

Las tecnologías biométricas constituyen un avance más en la sociedad digital, que se ha extendido con amplitud en muchos sectores y que por sus características peculiares requieren una regulación pormenorizada. La utilización cada vez mayor de este tipo de datos puede alejar el riesgo que conlleva su empleo, por cierto, nada despreciable. Los datos biométricos pueden revelar aspectos de comportamiento y características fisiológicas de las personas que pueden constituir una amenaza para los derechos y libertades de los individuos. Además, el uso de los datos biométricos, como la huella digital, puede ser empleado sin que el interesado sea consciente de ello, lo que puede deslegitimar la recogida y el tratamiento de estos datos y provocar una intrusión en los derechos de los individuos. En este caso, sería más fácil utilizar los datos para finalidades diferentes si se almacenasen en ficheros de datos centralizados. El uso más extendido de los datos biométricos se centra en facilitar la **autenticación o comprobación** de una persona para permitir el acceso a sitios de trabajo, o a lugares, ya sean físicos o virtuales y hacerlo de una manera constante y formalizada. El GT29 ha analizado la aplicación de las normas de protección de datos a los datos biométricos para intentar una regulación uniforme y eficaz en todos los Estados miembros[49], porque los datos biométricos son datos de carácter personal en la medida en que permiten la identificación de una persona. Presentan además características peculiares, tal y como señala el GT29, pues son datos universales (los datos biométrico existen en todas las personas), son únicos, (pues para cada persona son diferentes) y son permanentes (pues, salvo circunstancias excepcionales, permanecen en la persona a lo largo del tiempo), características que hacen inequívoca la identificación/comprobación de una persona. Los datos biométricos pueden ser de dos tipos: fisiológicos y comportamentales. Entre los primeros encontramos la voz, el iris, la huella dactilar, el reconocimiento facial, la detección del olor corporal, la retina, etc., que permiten la identificación/comprobación física de una persona. Entre los segundos destacamos la forma de caminar, determinados gestos, la firma, etc., que valoran aspectos del comportamiento de una persona. En este análisis nos centraremos en los datos biométricos fisiológicos y en concreto en la huella dactilar, por ser el más extendido.

[49] Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003, disponible en www.europa.eu.int/comm/privacy

Para recoger los datos biométricos, la huella digital, se procede con un sensor técnicamente preparado para captar el dato biométrico. Es la fase de la inscripción. A partir de la captación del dato se crea una plantilla que es "una reducción estructurada de una imagen biométrica: la medida biométrica registrada de una persona" (GT29). La plantilla es el elemento que forma parte del registro de datos, almacenada en forma digitalizada. A partir del registro de la plantilla disponemos, por ejemplo, de la huella digital para reconocer a la persona, pero hasta dicho momento, es decir, en la fase de inscripción podemos llegar a disponer de un elevado número de datos de carácter personal. Para identificar al sujeto por medio de una huella digital será necesario que este dato biométrico se compare con las plantillas ya almacenadas de otras personas y cuyos datos personales están registrados. De esta manera podremos verificar la identidad de la persona. Ahora bien, el GT29, que defiende el criterio de la proporcionalidad en el tratamiento de este tipo de datos, ha señalado que sería deseable "no almacenar la biometría en una base de datos sino más bien solo en un objeto disponible exclusivamente para el usuario, como una tarjeta con microchip, un teléfono móvil o una tarjeta bancaria", es decir, los tratamientos de datos biométricos para identificación/autenticación de la persona se pueden llevar a cabo sin proceder a un almacenamiento centralizado de datos biométricos o una memorización de los datos en manos diferentes de la persona, o sin utilizar excesivas técnicas de identificación.

La huella digital constituye un **dato biométrico de carácter personal**, según la definición de dato biométrico que se recoge en el artículo 4.14 del RGPD. Dato biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Por tanto, a la huella digital se le aplica la legislación de protección de datos de carácter personal, salvo que el almacenamiento de la plantilla no permita al responsable del tratamiento identificar a la persona por a través de un medio razonable y proporcionado. Otra cuestión más, la huella digital constituye una **categoría especial de datos,** que es la expresión con la que el RGPD alude a los datos que disfrutan de una protección más reforzada que los datos de carácter personal, en atención a los delicado de la información que aportan,

especialmente relacionada con aspectos de la personalidad del individuo o con espacios de su derecho a la intimidad (datos sensibles o especialmente delicados, en terminología de las normas precedentes).

La regla general en relación con las categorías especiales de datos, entre ellos, la huella digital, se contempla en el artículo 9.1 del RGPD, que prohíbe "el tratamiento de datos biométricos (…) dirigidos a identificar de manera unívoca a una persona física (…)". El apartado 2 del precepto contiene las excepciones que legitiman en tratamiento de huellas digitales. La entrada en vigor del RGPD reforzará las medidas de seguridad del tratamiento de huellas dactilares, puesto que frente a la legislación anterior, el derecho vigente a partir de la entrada en vigor del RGPD considerará especiales esta categoría de datos. Las excepciones al tratamiento de este tipo de datos se contemplan en el apartado segundo del precepto. Entre las que pueden afectar de manera más significativa a los datos biométricos y en especial a la huella digital podemos señalar: cuando el interesado haya dado su consentimiento para el tratamiento de estos datos; cuando el tratamiento es necesario para cumplir las obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, si lo autoriza el Derecho de la Unión o de los Estados miembros y se recojan las garantías adecuadas para el respeto a los derechos fundamentales e intereses del interesado; cuando el tratamiento sea necesario por razones de interés público esencial sobre la base del Derecho de la Unión o de los Estados miembros, que ha de ser proporcional al objetivo perseguido, respetar el derecho a la protección de datos y fijar medidas adecuadas para proteger los derechos fundamentales e intereses de la persona; para el tratamiento con fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia sanitaria o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social sobre la base del Derecho de la Unión o de los Estados miembros o por contrato con un profesional sanitario; cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencias sanitaria y de los medicamentos o productos sanitarios. Además, el considerando 53 prevé que los

Estados miembros pueda establecer otras condiciones de tratamiento, incluidas limitaciones para los datos biométricos, entre otras categorías de datos.

Mientras, el tratamiento de este tipo de datos personales se ha de ajustar a lo dispuesto en la LOPD. El sometimiento a la normativa de protección de datos exige que el tratamiento de las huellas dactilares cumpla con los requisitos de proporcionalidad del artículo 4.1 de la LOPD, Este precepto señala que solamente se podrán recoger datos de carácter personal para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, esto es, respetando el criterio de la proporcionalidad. La misma regla contiene el artículo 5.1.b y 5.1.c del RGPD. Esta última norma recoge, en el artículo 5.1.f, la necesidad de que los datos sean tratados de forma que se garantice la seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la adopción de medidas técnicas u organizativas adecuadas. Por tanto, la finalidad del tratamiento tiene que ser clara y la proporcionalidad entre los fines y los datos biométricos que se solicitan deben cumplirse, con el fin de provocar la menor lesión en los derechos y libertades de los individuos. La finalidad inicial del tratamiento impediría tratar los datos biométricos para otros fines distintos de los que motivaron la recogida. Por ejemplo, si se utiliza la huella dactilar para el acceso en hora al trabajo, no podría luego emplearse para controlar al trabajador en su puesto de trabajo. El principio de la finalidad impediría la reutilización de este tipo de datos, salvo que el interesado consintiera en ello. Las autoridades encargadas de la protección de datos analizan específicamente el criterio de la proporcionalidad en relación con los fines para valorar la legitimidad de un tratamiento de datos biométricos, pues, si aquellos pueden alcanzarse por medio del tratamiento de otros datos personales menos intrusivos, debe descartarse el tratamiento de los datos biométricos. Como decíamos más arriba, el GT29 considera un riesgo mayor para los derechos y libertades almacenar la plantilla de la huella digital en una terminal o en una base de datos central. Pero si se opta por este tipo de sistema, se debería elevar la propuesta a las autoridades de protección de datos, según la legislación de los Estados miembros.

El tratamiento de datos biométricos debe contar con las medidas de seguridad adecuadas desde el primer momento, esto es, desde el instante de la fase de inscripción. Las medidas de seguridad deben preservar la integridad de los datos, su confidencialidad y disponibilidad por el tercero legitimado que deba acceder a ellos. La pérdida de alguna de estas características podría hacer que estos datos estuvieran disponibles para otra persona, por ejemplo, si las huellas dactilares se asociaran a la identidad de otra persona y no permitieran al acceso a los servicios de que disfruta el sujeto a quien pertenecen las huellas digitales. El ejemplo servido ofrece una idea de las consecuencias que un error en el tratamiento de los datos biométrico puede tener para los derechos de los sujetos.

La utilización de los datos biométricos puede servir para reforzar la protección de los derechos de los individuos en la sociedad digital, siempre que el empleo de datos biométricos pueda reducir el tratamiento de otros datos de carácter personal. El GT29 recomienda establecer un diálogo entre los sectores que más ampliamente han comenzado a introducir el tratamiento de datos biométricos, estos son, el empleo, los visados y la inmigración y los transportes, y las partes interesadas, entre ellas las autoridades de protección de datos, con el fin de establecer códigos de conducta y directrices comunes para este tipo de tratamientos.

G. Derecho de oposición y decisiones individualizadas

El derecho de oposición puede ejercerse por motivos relacionados con la situación particular del interesado, debiendo cesar el tratamiento de los datos realizado por el responsable, salvo que se acredite un interés legítimo o sea necesario para el ejercicio o defensa de reclamaciones. Asimismo, puede ejercerse cuando el tratamiento tenga por objeto la mercadotecnia directa (art. 21 RGPD).

El interesado tiene derecho a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que determinados datos personales que le conciernan sean objeto de un tratamiento basado en “el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”, o bien cuando “el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o

por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño", incluida la elaboración de perfiles.

En estos supuestos, el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite "motivos legítimos imperiosos" para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan (art. 21, apartados 2 y 3, RGPD), incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

A más tardar en el momento de la primera comunicación con el interesado, la atención del derecho de oposición será informada explícitamente al interesado y será presentada claramente y al margen de cualquier otra información (art. 21.4 RGPD).

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público (art. 21.6 RGPD).

El artículo 18 del PLOPD reconoce este derecho por vía de remisión al propio RGPD. Por ejemplo, en un procedimiento selectivo de acceso a la Administración Pública, un aspirante que ha sido víctima de violencia de género puede instar la no publicación de sus datos personales, adoptándose las medidas técnicas para que esa información no sea publicada en Boletines Oficiales ni indexada por los buscadores.

También sería posible que un ciudadano ejercitase el derecho de oposición al tratamiento alegando:

- La elección indebida, por parte del responsable del tratamiento, de una forma de publicación de los datos personales que suponga un mayor nivel de publicidad del que dicho afectado deba soportar en atención a las circunstancias concurrentes, siempre que una Ley no disponga lo contrario.
- La publicación por parte del responsable del tratamiento de datos excesivos en atención a la tipología de los mismos y al especial nivel de protección dispensada por el ordenamiento jurídico a los datos personales publicados, siempre que una Ley no disponga lo contrario.
- El mantenimiento de la publicación de los datos personales por parte del responsable del tratamiento cuando dicha publicación haya dejado de ser necesaria o pertinente para los fines para los cuales se haya realizado.

Ante "publicidad institucional" remitida por una administración pública sería también posible el ejercicio del derecho de oposición al tratamiento, sin necesidad de que el ciudadano afectado especificara ningún motivo concreto.

Finalmente, en caso de ejercicio del derecho de oposición por un afectado al tratamiento de sus datos personales con fines de investigación y estadísticos, la excepción al mismo sólo puede basarse en claras razones de interés público.

Una manifestación especial del derecho de oposición es el derecho a no ser objeto de decisiones individualizadas basadas únicamente en tratamientos automatizados que se recoge en el artículo 22 del RGPD. Todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de su información de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Las excepciones a este derecho se concretan en los supuestos en que dicho tratamiento sea necesario para la celebración o ejecución de un contrato, esté permitido por el Derecho de la UE o de los Estados miembros -con medidas

adecuadas para salvaguardar los derechos y libertades del titular de los datos-, o bien exista consentimiento explícito del titular de los datos.

H. Limitaciones del ejercicio de los derechos

El RGPD establece una serie de limitaciones del ejercicio de los derechos de los interesados, cuyo alcance se concreta en una serie de excepciones al ejercicio de los derechos del Capítulo III del propio RGPD, y de los principios recogidos en su artículo 5 –dentro del Capítulo II-, en cuanto se vinculen a dichos derechos.

El artículo 23 del RGPD señala los supuestos que justifican las limitaciones del ejercicio de los derechos, cuya existencia debe estar amparada por el Derecho de la UE o por una norma con rango de ley. Asimismo, se exige que se trate de una medida necesaria y proporcionada en una sociedad democrática para el logro de los objetivos, fijándose expresamente –en el apartado 2-, el contenido mínimo de dicha disposición para asegurar el establecimiento de las garantías adecuadas:

> "1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22.
> En todo caso, dicha limitación debe respetar en lo esencial los derechos y libertades fundamentales, y debe tratarse de una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:
>
> a) la seguridad del Estado;
> b) la defensa;
> c) la seguridad pública;
> d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
> e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
> f) la protección de la independencia judicial y de los procedimientos judiciales;
> g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);
i) la protección del interesado o de los derechos y libertades de otros;
j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:
a) la finalidad del tratamiento o de las categorías de tratamiento;
b) las categorías de datos personales de que se trate;
c) el alcance de las limitaciones establecidas;
d) las garantías para evitar accesos o transferencias ilícitos o abusivos;
e) la determinación del responsable o de categorías de responsables;
f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;
g) los riesgos para los derechos y libertades de los interesados, y
h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta."

3.7. Relaciones entre el responsable y el encargado del tratamiento

Para estudiar las relaciones entre el responsable del tratamiento y el encargado de tratamiento en el ámbito de las administraciones públicas, debemos partir, en primer lugar, de las definiciones que al respecto establece el artículo 4.7 del RGPD.

- "Responsable del tratamiento" o "responsable": "La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".
- "Encargado del tratamiento" o "encargado": "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

La relación entre responsable y encargado aparece en la Administración Pública generalmente a través de una encomienda de gestión, un convenio o contrato administrativo.

En este último caso, la Disposición Adicional 26ª del texto refundido de la Ley de Contratos del Sector Público, Real Decreto Legislativo 3/2011 de 14 de noviembre, determina que "para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento".

El contenido mínimo del contrato contendrá el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Los considerandos 79, 81 y 95 así como el Capítulo IV del RGPD y el Título V del PLOPD, detallan las relaciones entre ambos, señalando que es deber del responsable la diligencia en la contratación del encargado.

En particular, el contrato o acto jurídico de encargo de tratamiento deberá contener:

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad.
- Las medidas de seguridad.
- El régimen de la subcontratación.
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los interesados.
- La colaboración en el cumplimiento de las obligaciones del responsable.
- El destino de los datos al finalizar la prestación.

La adhesión del encargado del tratamiento a un código de conducta o mecanismo de certificación podrá utilizarse como elemento para demostrar la existencia de garantías suficientes.

En virtud de lo dispuesto en la Disposición transitoria quinta del PLOPD los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta transcurridos 4 años desde la citada fecha.

En caso de que los contratos previesen su prórroga al término de su vencimiento deberá producirse su adaptación con anterioridad al momento en que estuviese prevista dicha prórroga.

Para facilitar esta labor de adecuación, la AEPD ha publicado el documento "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento", que contiene un Anexo con un ejemplo de cláusulas contractuales para aquellos supuestos en que el encargado del tratamiento trate los datos en los locales del responsable.

3.8. El Registro de actividades de tratamiento y el inventario de actividades de tratamiento

A partir del 25 de mayo de 2018, fecha en que el RGPD será aplicable, desaparecerá la primera de las obligaciones que al amparo de la LOPD debía realizar el responsable del tratamiento de datos de carácter personal: la notificación de ficheros ante la Agencia Española de Protección de Datos.

Si bien esta inscripción de ficheros desaparece, el RGPD regula en su artículo 30 el Registro de actividades de tratamiento de la siguiente forma:

> "1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
>
> a. el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
>
> b. los fines del tratamiento;
>
> c. una descripción de las categorías de interesados y de las categorías de datos personales;
>
> d. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
>
> e. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las

transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 13.

2. (…)

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10."

Entre las novedades respecto del contenido de la actual notificación de ficheros destacan la información sobre los plazos previstos para la supresión de las diferentes categorías de datos y la identificación del Delegado de Protección de Datos.

El artículo 31.2 del PLOPD establece que ciertos sujetos (entre los que se encuentran los órganos constitucionales) "harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal."

3.9. La seguridad en el RGPD

El derecho fundamental a la protección de datos no es protegible si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

Para garantizar la confidencialidad deben adoptarse medidas que impidan el acceso no autorizado a los datos personales, que eviten la vulneración del deber de secreto y que garanticen los privilegios de acceso a la información o los datos personales (a través, por ejemplo, de la gestión de las altas, bajas y asignación de roles en los sistemas informáticos del personal de una organización).

La integridad de los datos personales o de la información se relaciona con el principio de exactitud o de calidad de los datos. De acuerdo con este principio, el responsable del tratamiento de los datos debe garantizar que son acordes a la realidad y adecuados a la finalidad para la que fueron obtenidos y, además, garantizar su inalterabilidad.

La disponibilidad, por su parte, permite mantener los datos accesibles para su consulta, localización y rectificación cuando sea necesario. Esta característica garantiza los derechos de acceso, rectificación, supresión, derecho de limitación del tratamiento y portabilidad.

A. Evaluación del riesgo y medidas de seguridad

El artículo 32 del RGPD establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento así como los riesgos de probabilidad y gravedad para los derechos y libertades de las personas.

Corresponderá al responsable del tratamiento, previa evaluación del riesgo (que incluye la valoración del impacto de los tratamientos de datos para los derechos y libertades de las personas afectadas), determinar las medidas de seguridad que sean necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, así como la continuidad de los sistemas y servicios de tratamiento y la restauración de la normalidad en caso de incidente. Las medidas de seguridad que se definan deben ser aplicadas tanto por el responsable como por el encargado del tratamiento.

Otras figuras clave son las del responsable de seguridad, encargado de implantar las medidas de seguridad, y el Delegado de Protección de Datos, con funciones de asesoramiento.

La implantación de las medidas de seguridad, como señala la Disposición adicional primera del PLOPD, se ajustará a lo establecido en el Esquema Nacional de Seguridad. Esta previsión es acorde con la más genérica contenida en el artículo 17.3 de la LPACAP en relación con cualquier información en poder de las AAPP: "los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos".

Una descripción general de las medidas de seguridad adoptadas en cada tratamiento, a través de la enumeración de medidas o por referencia a otras normas o procedimientos adoptados, debe incorporarse al Registro de actividades de tratamiento y publicarse en el Inventario de actividades de tratamiento.

La AEPD ha publicado una "Guía para una evaluación de impacto en la protección de datos personales", que plantea una metodología de análisis y gestión de riesgos.

Una de las medidas que pueden contribuir a reducir el nivel del riesgo es la seudonimización. La seudonimización o disociación de los datos personales supone eliminar aquellos datos que a priori permiten una identificación de los interesados, dejando accesibles aquellos datos o información personal que se necesita para el tratamiento. Se trata de un mecanismo que oculta la identidad de los interesados pero este ocultamiento de la identidad es reversible y siempre podremos reidentificar a las personas (frente a la anonimización, que no permite la reidentificación de los interesados).

Otro elemento de seguridad esencial es el que permite identificar unívocamente a las personas o procesos que acceden a la información y las acciones que han realizado (trazabilidad).

B. Gestión del riesgo

Analizar el riesgo no serviría de nada si posteriormente no se realiza un esfuerzo para evitarlo o reducirlo. A esta actividad se la denomina "gestión del riesgo".

Un análisis de riesgo es una actividad sistemática por la que se pretende identificar cada uno de los riesgos implícitos en una determinada actividad. Los riesgos no son estáticos, evolucionan según el estado de la tecnología y las situaciones específicas de cada tratamiento de datos personales, cada organización debería tener una política de riesgos corporativa o un marco en el que se identifique a los responsables del análisis, los recursos, los procesos, los activos, la metodología necesaria para realizar el análisis de riesgos, las herramientas necesarias, la gestión del riesgo, la periodicidad de los análisis, las medidas de seguimiento, las legislaciones aplicables, la formación del personal, etc.

Para poder establecer el marco de referencia del análisis y la gestión del riesgo en una organización, pueden utilizarse normas y metodologías como las siguientes:

- Las normas ISO 31000 Y 31010 pueden servir de ayuda para configurar el marco de referencia para el análisis de riesgos en general.
- La norma ISO 27005 puede utilizarse como marco para el análisis de riesgos para la seguridad de la información.
- La metodología MAGERIT de análisis y gestión de riesgos, elaborada por el Consejo Superior de Administración Electrónica, también puede ser de utilidad.

C. Notificaciones de brechas de seguridad

Es obligación del responsable del tratamiento (y del encargado, en su caso), la notificación de las violaciones de seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados, o la comunicación o acceso no autorizado a dichos datos, siempre que exista

riesgo para los derechos y libertades de las personas físicas, riesgo que ha de ser evaluado por el responsable.

El artículo 33 del RGPD se refiere a las obligaciones de notificación del responsable a la Autoridad de Control, y el artículo 34 a las obligaciones de notificación al interesado.

La notificación de la brecha a la autoridad de control se ha de producir antes de las 72 horas siguientes al conocimiento por el responsable de la existencia de la violación. Pero la norma deja abierta la posibilidad de una notificación más allá de las 72 horas, si se adjunta una justificación del porqué de dicha dilación.

La comunicación de la violación a la Autoridad de Control va más a allá de la mera indicación de que la brecha se ha producido. El RGPD detalla un conjunto de datos que es obligado describir como mínimo:

- Naturaleza de la violación de la seguridad de los datos personales. Para describir la naturaleza hay que incluir, siempre que sea posible:
  - Las categorías de interesados afectados
  - El número aproximado de interesados afectados.
  - Las categorías de datos comprometidos.
  - El número aproximado de registros de datos personales afectados.
- Nombre y datos de contacto del Delegado de Protección de Datos o, en su caso, de otro punto de contacto en el que pueda obtenerse más información.
- Posibles consecuencias de la violación de la seguridad de los datos personales.
- Medidas correctivas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales.

El responsable ha de implantar un procedimiento documentado de gestión de las violaciones de seguridad. Ese procedimiento registrará todos los hechos relacionados con la violación, lo que implica que se anotará no sólo la información anteriormente

señalada sino cuándo, cómo y dónde se ha producido la brecha, el personal o entidades implicadas, los sistemas afectados, etc.

La notificación de la brecha de seguridad a los interesados no tiene un plazo temporal establecido en el RGPD, sólo se señala que esta ha de producirse cuanto antes, teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. El objetivo de esta notificación es que el interesado pueda conocer las implicaciones de lo que ha pasado y qué medidas personales puede adoptar para proteger sus derechos. Por lo tanto, ha de ser una información eminentemente práctica.

El RGPD establece una serie de excepciones a la necesidad de comunicar la violación a los interesados cuando:

- El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, lo que sucede si los datos están cifrados.
- El responsable ha tomado medidas ulteriores que garanticen que ya no existe la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado.
- Si realizar esa comunicación supone un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública por la que se informe de manera igualmente efectiva a los interesados.

Hay que tener en cuenta que la decisión del responsable de no notificar a los interesados puede ser revocada por la Autoridad de Control y ésta exigir que dicha notificación se realice.

Por otro lado, el artículo 40, relativo a códigos de conducta, permite establecer condiciones de aplicación de la obligación de comunicación de las brechas de seguridad para las entidades adheridas a los mismos.

4. Obligaciones de los ciudadanos en la sociedad digital

Mucho se habla sobre derechos digitales, y poco de obligaciones. En ningún caso deben olvidarse estas últimas, puesto que suponen un componente esencial en el concepto mismo de derechos.

En poco más de 40 años se está produciendo la transformación de las empresas, de la Administración Pública y de la sociedad en general. En cada uno de estos grupos de actores nos detendremos.

4.1. Obligaciones de las empresas

En relación a la protección de datos, y teniendo en cuenta todo lo expuesto anteriormente, las empresas son titulares de nuevas obligaciones relacionadas con su desempeño en la nueva sociedad digital.

En primer lugar, las empresas deben respetar el contenido de la normativa de protección de datos en general. En el momento de la creación de ficheros de datos personales, han de respetar las normas de creación, organización y funcionamiento del fichero. Además, como ya hemos comentado, rigen para los ficheros gestionados por empresas las siguientes reglas:

Seguridad de los datos

La ley establece esta obligación para el responsable del fichero. Han de adoptar medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Las medidas de seguridad se contemplan en los artículos 25 y 33 del RGPD. En el artículo 25 se contemplan las medidas de seguridad desde el diseño y por defecto, de

las que ya hemos hablado y que suponen el establecimiento de medidas desde el inicio del tratamiento y prolongándolas durante todo el tiempo que se continúe con dicho tratamiento. El artículo 32 del RGPD señala elementos que van a determinar la implantación de las medidas de seguridad adecuadas para la protección de los derechos y libertades del sujeto. Entre las medidas se incluyen al seudonimización, y el cifrado de los datos, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento, la capacidad para restaurar la disponibilidad y el acceso a los datos, un sistema de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas que garanticen la seguridad del tratamiento. Entre las medidas de seguridad se contempla la adhesión a un código de conducta o a un mecanismo de certificación (art. 32.3 RGPD).

Deber de secreto

Este deber de mantener el secreto profesional respecto de los datos de carácter personal afecta no sólo al responsable sino a todos los que de algún modo intervengan en cualquier fase del tratamiento automatizado, es decir, incluye al encargado.

Comunicación de los datos

El que comunica y el que recibe los datos se obliga por el sólo hecho de la cesión a la observancia de la LOPD. Salvo procedimiento de disociación previo, los requisitos de toda comunicación de datos son: a) Que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. b) Consentimiento previo del interesado, salvo que cuente con autorización por ley, que los datos se recojan de fuentes accesibles al público, o que exista una relación jurídica entre efectuado y cedente, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión del fichero con ficheros de terceros. Así mismo, si el destinatario es el Defensor del Pueblo u órganos del Poder judicial, la cesión se produce entre administraciones públicas cuando tenga por objeto un tratamiento posterior de los datos con fines históricos, estadísticos o científicos, o se trate de datos relativos a la salud para solucionar una urgencia o para realizaran estudios epidemiológicos.

La comunicación de datos personales, en el marco de un acuerdo de encargado del tratamiento, a un país que no forme parte de la Unión se rige por la regulación establecida en el Reglamento para las transferencias internacionales. Este sería el caso de la contratación de servicios de *cloud computing* por parte de un responsable de la UE a una empresa establecida fuera de la Unión.

En lo que se refiere al responsable y al encargado del tratamiento, es preciso tener en cuenta que la mayor novedad que presenta el RGPD es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del RGPD, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación.

La figura del delegado de protección de datos adquiere una destacada importancia en el RGPD y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La AEPD mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. El responsable o el encargado deberán dotar al delegado de medios materiales y personales suficientes y no podrán removerle, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el

interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

Además, las empresas deberán garantizar el **derecho a la portabilidad**[50] en los términos establecidos en la legislación.

Existen también obligaciones relacionadas con las **transferencias internacionales de datos personales**. Las normas jurídicas, en su aplicación y eficacia, están sujetas a ciertos límites espaciales y temporales. Todos los principios y derechos reconocidos en la legislación de un país se ven amenazados si no se establece un control sobre los movimientos de datos que atraviesen una frontera (caso de las multinacionales, no salen de la misma persona jurídica): si el país receptor tiene menor nivel de protección que el de origen, los datos pueden ser tratados sin ninguna restricción legal y reenviados al origen, burlando así la aplicación de la legislación de este país (problemática de los paraísos de datos).

Existe, pues, la necesidad de que el nivel de protección existente en el país de origen y el de destino sea similar. A nivel de la UE, las diferencias existentes entre los Estados Miembros suponen un obstáculo para el desarrollo de la actividad económica y la libre circulación de personas y cosas.

El artículo 33 de la LOPD establece que la protección en el país de destino debe ser equiparable a la que presta la LOPD, salvo autorización previa de la AEPD. A estos efectos, el Ministro de Justicia, previo informe de la AEPD elaboró una lista de países que se entiende proporcionan un nivel de protección equiparable (el listado se encuentra en la web de la AEPD).

Existen algunas excepciones con base a aplicación de tratados internacionales (Schengen): cuando la transferencia se haga con el fin de prestar o solicitar auxilio judicial internacional, en el caso de los datos de carácter médico, o cuando se refiera a transferencias dinerarias, de acuerdo con su legislación específica.

[50] Paul De Hert, *et al*. (2017).

Según establece la Instrucción de la AEPD nº 1/2000, de 1 de diciembre, por la que se rigen los movimientos internacionales de datos, cualquier fichero que pretenda llevar a cabo transferencias internacionales de datos deberá hacerlo constar expresamente al proceder a la notificación del fichero al Registro General de Protección de Datos, con la excepción del artículo 34 de la LOPD.

Para el caso de las transferencias a EEUU regían los "Principios de puerto seguro". En 1995, la Directiva estableció una regla general para las transferencias de datos (la del art. 33 LOPD vista arriba), y en el año 2000, se estableció el principio de *Safe Harbour*, o Principios de Puerto Seguro. El Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, aquellos debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.

En 2013, el Comisionado de Protección de datos de Irlanda presentó una denuncia contra Facebook (que recibía datos de los europeos en virtud de los principios de puerto seguro). El TJUE estableció que los principios de *Safe Harbour* son nulos, por ser contrarios a los principios de protección de datos de la UE. Esto afectó a todas las empresas que hacían transferencias de datos hacia EEUU.

Este es el motivo por el que en la UE se llegó a un acuerdo político en el que se estableció un nuevo marco: el Escudo de Privacidad. Las obligaciones de las empresas sujetas al Escudo de Privacidad se derivan de los derechos de los ciudadanos:

a) Derecho a ser informado.

   Una empresa sujeta al Escudo de Privacidad deberá informarle sobre:

   - Los tipos de datos personales que procesa.
   - Los motivos por los que procesa sus datos personales.

- Si tiene intención de transferir sus datos personales a otra empresa, y por qué.
- El derecho a solicitar a la empresa que permita acceder a sus datos personales.
- El derecho a elegir si permite que otra empresa use sus datos personales de forma "sustancialmente diferente" o revelarlos a otra empresa (también conocido como el derecho de "exclusión voluntaria").
- Cuál es el órgano de resolución de controversias independiente, ya sea en la UE o en los EEUU, al que pueda presentar su caso.
- Cuál es el organismo público en el caso de los EEUU responsable de investigar y hacer cumplir las obligaciones de la empresa en virtud del marco normativo.
- La posibilidad que pudiese corresponderle a este de tener que responder a solicitudes de autoridades públicas estadounidenses de revelar por ley información acerca del usuario.

La empresa sujeta al Escudo de Privacidad deberá proporcionarle un enlace a su política de privacidad si dispone de sitio web público o bien un enlace al que pueda acceder en caso de que no disponga de este.

b) Limitaciones en el uso de sus datos para diversos fines.

La empresa sujeta al Escudo de Privacidad solo podrá recibir y procesar datos personales en la medida en que sean pertinentes para el propósito del tratamiento, debiendo garantizar que los datos usados sean exactos, fiables, completos y estén actualizados. Únicamente se permite guardar los datos personales en tanto resulten necesarios para el propósito del tratamiento. A dichas empresas se les permitirá conservar datos durante periodos más prolongados exclusivamente en caso de que los necesite para determinados fines en particular, tales como archivo por interés público, periodismo, literatura y arte, investigación científica o histórica, o para análisis estadístico.

c) Minimización de los datos y obligación de guardar los datos únicamente durante el tiempo necesario.

d) Obligación de asegurar los datos.

La empresa deberá garantizar que sus datos personales se guarden en un entorno seguro y se protejan frente a pérdida, utilización ilegal, acceso no autorizado, revelación, alteración o destrucción, teniendo en cuenta debidamente la naturaleza de los datos y los riesgos que conlleva el tratamiento.

e) Obligación de proteger los datos si se transfieren a otra empresa.
   Independientemente de su ubicación, si dentro o fuera de los EEUU, la empresa que recibe los datos deberá garantizar el mismo nivel de protección de sus datos personales que el otorgado por el marco del Escudo de Privacidad. Esto requiere la suscripción de un contrato entre la empresa sujeta al Escudo de Privacidad y el tercero que estipule las condiciones en las que este podrá usar sus datos personales y sus responsabilidades de protección de tales datos.
f) Derecho de acceso y rectificación de sus datos.
   Le corresponde el derecho a solicitar a la empresa sujeta al Escudo de Privacidad que le permita acceder a sus datos personales. Esto significa que tiene derecho a que le comuniquen sus datos, pero, además, a obtener información sobre el fin para el que se procesan los datos, las categorías de datos personales afectadas y los destinatarios a los que se les revelan los datos.
g) Derecho a presentar una reclamación y a obtener reparación.
   Si la empresa no cumple las normas del Escudo de Privacidad e infringe su obligación de proteger sus datos personales, se dispondrá del derecho a reclamar y obtener reparación, sin coste alguno.

Tal y como ya señalamos, las empresas tienen obligaciones con relación la **neutralidad de la Red**, tan necesaria para garantizar el acceso en condiciones de igualdad a las ventajas que ofrece Internet.

Del mismo modo, deberán respetar los principios relativos a la **accesibilidad electrónica**, aunque sólo las redes sociales de cierto tamaño tienen prescripción legal de respetar la accesibilidad electrónica.

El proyecto "Ranking Digital Rights"[51] establece una relación de empresas de telecomunicaciones e Internet en función de sus protocolos en el tratamiento de los derechos de los ciudadanos y sus vidas digitales. Tanto los gobiernos como las empresas tienen la obligación de proteger estos derechos. Es vital exigir trasparencia y responsabilidad en cuanto al tratamiento que hacen de la información de las

[51] https://rankingdigitalrights.org/

personas, y cómo garantizar su protección o cuáles son las medidas de seguridad que se implantan.

Por otro lado, los algoritmos son el elemento clave en la digitalización, selección y eliminación de contenidos. El análisis que hace el algoritmo de la información en principio busca un objetivo (mejorar experiencia como usuario), y se supone que es un interés legítimo, pero a veces se utiliza abusivamente. Las empresas utilizan los algoritmos como parte de su modelo de negocio, pero esto debe ser compatible con los derechos de las personas.

4.2. Obligaciones de los Estados

Una primera obligación de los Estados se refiere a la de **actualizar el ordenamiento jurídico** para que refleje toda la realidad del cambio tecnológico. Ante la necesidad de que el código penal dé cabida a todas las nuevas formas de delincuencia surgidas al amparo de las nuevas tecnologías, se ha llevado a cabo una reforma de este y de la ley de enjuiciamiento criminal que incluye medidas de investigación tecnológica para hacer frente a este nuevo escenario de "ciberdelincuencia". Por otro lado, las leyes de enjuiciamiento civil deben ser sometidas a un proceso de nueva generación que incorpore todo lo que ofrecen las nuevas tecnologías, pensando el derecho desde la tecnología. Junto a estos fenómenos se identifica una necesidad de universalización de la garantía de los derechos, que supere los estrictos límites territoriales.

Debemos aplicar los instrumentos internacionales de derechos humanos al mundo digital. El desarrollo de las políticas públicas que necesariamente deben acoger la transformación digital como herramienta al servicio del ciudadano en un modelo de humanismo tecnológico y debe tener en cuenta esta nueva dimensión de los derechos.

Es necesario **revisar los escenarios regulatorios y el diseño de políticas públicas**, cubrir lagunas y fijar condiciones básicas que permitan la transformación digital ordenada y eficiente, potenciando a la vez la innovación tecnológica y el libre ejercicio de los derechos de las personas.

Este es un esfuerzo que requiere un compromiso estable de cooperación de todas las partes implicadas: el sector público, el sector privado y la sociedad civil, para tratar de alcanzar estándares universales seguros.

La justicia española está totalmente fragmentada, por lo que se trabaja en la creación de un sistema de gestión procesal común que ofrezca mayor integración y conectividad. De la misma manera, la tecnología debe servir para una asignación de recursos más automatizada y eficiente.

Por otro lado, el concepto de justicia abierta es otro de los grandes retos a ser abordados. La reutilización de los datos en el ámbito de la justicia y la transposición de la directiva de protección de datos en materia judicial y penal son algunos de los desafíos a los que nos enfrentamos.

Asimismo, es fundamental la actualización de los recursos humanos y profesionales de la justicia que han de incorporar las competencias digitales a su ámbito, dándose un cambio cultural en un sector profesional de carácter más clásico.

Por otro lado, apostamos por una suerte de "interoperabilidad legal", un marco que haga posibles escenarios de compatibilidad entre normas nacionales diversas. Los distintos actores son conscientes de que hay acciones que emprender, pero cada actor debe emprender la tarea desde su enfoque y herramientas para construir después un diálogo común. Los Estados siguen ostentando el monopolio de la representación de la ciudadanía en el plano internacional. Deben cambiar las dinámicas nacionales antes de llegar a acuerdos internacionales. Al mismo tiempo cada ciudadano es un *stakeholder* potencial y las asociaciones civiles trasnacionales tienen la capacidad de interactuar y presionar a los gobiernos. De algún modo se define un nuevo ámbito en el que lo trasnacional sucede a lo internacional, que implicaba un diálogo sólo entre gobiernos.

Un modelo de humanismo tecnológico al servicio de los seres humanos supondría un reto importante. El cambio real debe producirse en las democracias nacionales; los

retos que plantea Internet deben afrontarse reinventando los gobiernos, o el gobierno a nivel nacional. Nuestras democracias no han cambiado sustancialmente en el último siglo y deben hacerlo ya desde distintos puntos de vista, en los servicios, en el diseño de políticas públicas, en el diálogo con expertos y compañías. Los gobiernos deben aprender, e incluso copiar, de la estructura trasnacional de Internet. En este sentido, la dimensión del compromiso político iría en el siguiente sentido: 1) fomento de un mayor debate y compromiso y 2) formación, adquisición de un conocimiento profundo sobre Internet antes de regular.

Por otro lado, a pesar de la trasnacionalidad, los conflictos deben ser siempre contextualizados. Cada continente, cada territorio incorpora elementos propios que definen un contexto, lo que dificulta la labor de las compañías, pues operan en marcos jurídicos diversos y deben aplicar la normatividad vigente. Además, parece que el derecho siempre va por detrás de la tecnología y las regulaciones detalladas no son buenas o resultan obsoletas. Lo esencial, desde el punto de vista corporativo, es disponer de políticas de transparencia pública, *Law Enforcement Report*, que permitan al público conocer su actuación.

Con respecto a la **protección de datos personales**, las Administraciones pueden desarrollar tratamientos de datos personales cuando los precisen para el cumplimiento de las funciones que el Ordenamiento Jurídico les ha atribuido. El artículo 6 del RGPD contempla la licitud del tratamiento "cuando es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento". Respecto de los tratamientos de datos de las administraciones públicas se han introducido notables restricciones al ejercicio de los derechos de información, acceso, rectificación y cancelación, así como en relación a los datos sensibles.

4.3. Obligaciones de los ciudadanos

Resulta muy relevante detenerse en las obligaciones de los ciudadanos, que acompañan a los derechos que hemos desarrollado. En primer lugar, el deber general de respeto a los derechos de terceras personas en el ámbito digital. Por otro lado, es exigible a los mismos un comportamiento ético y jurídicamente responsable en el

mundo digital. Lo cual tiene innumerables matizaciones, puesto que abarca desde la privacidad, hasta la propiedad intelectual, la libertad de expresión responsable, etc.

Los ciudadanos deben ser diligentes en la adopción de medidas de seguridad en el uso de Internet y nuevas tecnologías. Esto afecta a particulares y empresas, que están legalmente obligadas a tomarse en serio la seguridad, habida cuenta de que es el único medio que garantizará, entre otras cosas, la privacidad del individuo.

Además, hay que recordar la obligación de respeto a la ley de protección de datos en lo que respecta al uso de información personal perteneciente a personas físicas, así como la obligación de respeto a la Ley de Propiedad Intelectual en cuanto al uso y posible aprovechamiento de los contenidos digitales de los que el sujeto no sea autor.

Existe asimismo un deber general de transparencia como principio esencial en Internet. Y por supuesto, una obligación de respeto a las normas de accesibilidad electrónica.

Por otro lado, los ciudadanos deben reportar o notificar a la autoridad –a la mayor brevedad- en caso de delitos.

La educación y diálogo entre gobiernos, sector privado y sociedad civil es clave para mejorar la comprensión de las potencialidades de Internet. Los niños, como nativos digitales, serán los grandes protagonistas de los cambios. Ellos cubrirán las brechas de demanda y por tanto hay que centrarse en las escuelas para fomentar una sociedad digital.

5. Ética y tecnologías emergentes: códigos de conducta

5.1. Introducción

La digitalización progresiva y a gran velocidad de nuestra actividad (económica, social, cultural, etc.) ha dado lugar a una agenda comunitaria y nacional que pretende impulsar políticas públicas que permitan responder a los retos que se presentan.

La Agenda Digital para Europa fue concebida como una de las siete iniciativas de la Estrategia Europa 2020 adoptada por la Comisión. La Agenda Digital para España establece una hoja de ruta en materia de Tecnologías de la Información y las Comunicaciones (TIC) y de administración electrónica tal y como ya hemos comentado.

Este marco político se está demostrando insuficiente para garantizar los derechos digitales de la ciudadanía. En este trabajo nos centraremos en los **retos éticos y jurídicos**, puesto que partimos de la convicción de que ambos son necesarios y complementarios, y en ningún caso, suficientes para afrontar la magnitud de los desafíos. Es necesario reforzar el marco de los principios éticos y el de los retos jurídicos, promoviendo un debate público y unas adaptaciones legislativas expuestas en el punto 1 de este informe.

Algunos de los principios éticos que se recogen en los códigos deontológicos[52] consultados son: rigor profesional; diligencia en el desempeño de la profesión; Actualización; objetividad; evaluación de riesgos; honestidad e integridad; prevención de la corrupción; respeto a la vida, a la ley y al bien común; seguridad; liderazgo responsable. Si se aplican estos principios a las tecnologías emergentes, los retos que se plantean son numerosos.

[52] Los códigos que mejor describen las implicaciones éticas de las nuevas tecnologías son los del IEEE y ACM. Institute of Electrical and Electronics Engineers - IEEE (2017): *Code of Ethics*. http://www.ieee.org/about/corporate/governance/p7-8.html

Algunos autores presentan el concepto de “vida exponencial”, que supone una visión, forzosamente parcial y esquemática, del potencial de las llamadas tecnologías exponenciales y sus implicaciones económicas, sociales, medioambientales, éticas e, incluso, ontológicas.

Según esto, la humanidad se encuentra en los inicios de una revolución tecnológica de desarrollo acelerado, en comparación con otras anteriores, y de un alcance tal que va a generar transformaciones que solo comenzamos a imaginar. Porque las tecnologías que están emergiendo van a cambiar —están cambiando ya— lo que parecían constantes fundamentales de la naturaleza humana: hoy parece posible mejorar drásticamente la memoria de las personas, sus procesos cognitivos, sus capacidades físicas e intelectuales, y aumentar la longitud de su vida hasta extremos que pueden cambiar nuestro concepto de mortalidad. Junto con las inmensas posibilidades que todo esto supone, plantea también incógnitas muy relevantes para la especie humana.

Los avances recientes y las perspectivas de desarrollo en las biociencias, la genética, en la robótica y en la inteligencia artificial, y en la construcción de esa red global de sensores interconectados que se ha dado en llamar Internet de las cosas son los temas que supondrán una parte de esta revolución.

> “Los avances científicos y tecnológicos ofrecen increíbles posibilidades de aumento de la renta y el bienestar, pero también conllevan enormes riesgos, que van desde la posibilidad de un crecimiento drástico del desempleo y la desigualdad, o de presiones insoportables sobre los sistemas de protección social, hasta amenazas catastróficas para el planeta y para la supervivencia de nuestra especie.
> Sin embargo, la propia tecnología nos ofrece nuevas y mejores posibilidades para conjurar estos riesgos. Orientar el desarrollo científico y tecnológico hacia la mejora efectiva de las condiciones de vida de todos, y hacia la sostenibilidad, exige una actualización de nuestros esquemas éticos que nos ayude a actuar de forma responsable en un entorno distinto de todo lo que hemos conocido y rápidamente cambiante. Un entorno en el que se abren perspectivas absolutamente nuevas para la especie humana, como la transición hacia una «era poshumana» donde las personas, con capacidades enormemente aumentadas, convivan con «inteligencias artificiales» superiores a la humana y capaces de reproducirse autónomamente generando descendencia aún más inteligente

> —lo que se ha llamado «la singularidad»—. O la posibilidad, cada vez más cercana, de la expansión de los humanos —o poshumanos—.”[53]

El propósito de la tecnología es mejorar la vida de las personas. Esto implica que las tecnologías se desarrollan con particulares valores en mente, como la eficiencia. Esto se ha defendido por parte de muchos autores (Nissebaum; Winner). En otras palabras, la tecnología no es neutral en lo que respecta a valores. Se habla incluso de que, dependiendo del desarrollo tecnológico y como sea este, el usuario está predispuesto a determinados valores[54].

Cada día aumentamos nuestra huella digital a través del uso continuado y frenético de las TIC: accesos a nuestro teléfono móvil, localización GPS en coche y móvil, listados de amistades en redes sociales, justificantes de compras online, voluminosos textos y archivos compartidos por correo electrónico y mensajes de texto. Hasta ahora, esta información permanecía en bases de datos separadas e inaccesibles como un conjunto. Sin embargo, los proveedores se han dado cuenta del potencial que supone almacenar y compartir la máxima cantidad de información. Piénsese, por ejemplo, en las aplicaciones del *big data*. De esta forma, hacer un seguimiento de nuestra huella digital es mucho más sencillo. Las empresas de marketing digital podrán hacernos ofertas mucho más personalizadas. Pero, ¿cuál es el precio que estamos pagando por ello?

Una mayor conciencia en torno a nuestros derechos como ciudadanos en el mundo de la información es analizada por Luciano Floridi, que argumenta que la información tiene una fuerza ontológica en la construcción de nuestra identidad personal, trayendo consigo, en el nivel más profundo, que la información afecta a quiénes somos y qué podemos llegar a ser. No debemos renunciar a ciertos derechos para poder seguir siendo quienes somos.

Lori Andrews nos recuerda que Facebook está redefiniendo el contrato social: está haciendo lo privado público, y al revés. En este momento, debemos analizar cómo se puede mantener la protección de los ciudadanos; qué reglas debieran gobernar lo que

[53] BBVA (2016).

[54] John Sullana, *Rights and computer ethics*.

se puede hacer o no con nuestros datos; nuestros derechos, etc. Y todo ello, en un momento en que está en cuestión el proceso político mismo.

Están apareciendo en la Red nuevas normas que son distintas a las normas offline (piénsese en el caso de aquel juez recusado por mantener amistad a través de una red social con un abogado en la causa que debía decidir).

Los padres de la Constitución americana se aseguraron de que los derechos no pudiesen cambiarse sin previo aviso, pero hoy día las redes sociales modifican sus cláusulas sin que el usuario pueda reaccionar.

La propia estructura de las redes sociales impide que cualquiera pueda reinventarse o empezar de nuevo. Basta con recordar lo difícil que es, por el momento, ejercer el derecho al olvido que el Nuevo reglamento Europeo de Protección de Datos reconoce.

Otra cuestión que está pendiente es el concepto de *collective privacy* (privacidad de grupos de personas) y la necesidad de que nuestras leyes se adapten al panorama tecnológico para proteger bien la privacidad, dado que una mayor parte de nuestra vida se desarrolla ahora online.

Según un estudio reciente[55], "tres de cada cuatro españoles considera que la expansión de los teléfonos inteligentes y su uso intensivo produce situaciones antisociales y de aislamiento. El 71,1% reconoce cierta dependencia de la tecnología, mientras que más de la mitad de los españoles comulgan con la creencia de pérdida de reflexión por el exceso de información y con la pérdida de valor de los contenidos por efecto de su enorme disponibilidad. En cuanto a los problemas de la intimidad y la privacidad tan mencionados en relación a Internet, es clara la posición de los españoles: menos de un 20% considera que la privacidad e intimidad estén bajo control en Internet".

[55] ONTSI (2017b:59)

Por otro lado, Castells (2000) recuerda que tanto las redes de información como la información que ellas contienen escapan, en muchas ocasiones, a las regulaciones nacionales e internacionales. Nos referimos aquí al espinoso tema de la jurisdicción aplicable a los innumerables problemas que se plantean a diario en relación a los datos que viajan por redes telemáticas.

En general, puede decirse que, tras la progresiva transformación digital, no existe actualmente nadie con una imagen completa de quién ha estado recopilando datos y de quién. La NSA en EEUU cuenta con mucha información, pero aún se le escapan muchos algoritmos que empresas y gobiernos aplican a datos personales continuamente. Por este motivo, algunos autores (J. Lanier) plantean la posibilidad de que los datos personales se monitoricen, lo cual es una idea que está valorándose con diversas formas en algunas empresas. Esta solución no nos parece en absoluto respetuosa con los derechos fundamentales, puesto que supondría una renuncia de los derechos por parte de los ciudadanos a cambio de un precio, lo cual iría contra los principios esenciales de los derechos humanos.

Cuando nos referimos a tecnologías emergentes estamos pensando en el "Internet de las cosas", *big data*, *cloud computing*, RFID, drones, robots, sistemas de videovigilancia, etc. Todas ellas plantean retos, principalmente en el derecho a la protección de datos, puesto que el consentimiento del afectado no suele darse. En el caso de la videovigilancia, se han utilizado tres sistemas para hacer compatible la privacidad, con la seguridad: la regulación, la auto-regulación y el diseño de protecciones dentro de los sistemas tecnológicos. Sin embargo, la realidad supone una extensión de estos sistemas en todos los ámbitos de lo que serán las *smart-cities*, sin que el individuo vaya a poder defender apropiadamente sus derechos.

En general, la introducción de nuevas tecnologías crea nuevas situaciones sociales en las que los individuos deben decidir cómo comportarse. En estas nuevas situaciones, los individuos no tenemos tiempo de desarrollar colectivamente normas que guíen nuestro comportamiento. El rápido crecimiento de las tecnologías de la información y las comunicaciones nos han llevado a una serie de circunstancias en las que no está claro cuáles son las normas y el alcance del consentimiento. ¿Debería este

consentimiento darse antes de que una fotografía que contiene nuestra imagen es convierta en un post en Internet? Con la ley española como marco, la respuesta es sí. Pero la realidad va por otros derroteros.

A continuación, sintetizamos algunas de las preocupaciones que generan las tecnologías más novedosas y que más influencia e impacto tendrán en nuestra sociedad en los próximos años. La mayoría están relacionadas con el asunto de la privacidad, y de la forma en cómo los ciudadanos estamos perdiendo el control sobre la información personal que nos concierne. Esto es muy preocupante en el caso del *big data*, dado que, a priori, no puede saberse mientras se utiliza esta tecnología, qué tipo de información va a conseguirse, o qué tipo de conclusiones se derivarán. De esta forma, es muy difícil solicitar el consentimiento antes de comenzar el tratamiento, siendo este un requisito esencial para poder llevarlo a cabo. En el caso de la robótica, las preocupaciones están relacionadas con la pérdida de control por parte del individuo, y las posibles consecuencias que la vida del robot pueda traer consigo. Si un vehículo autónomo atropella a una persona, ¿a quién se podrá hacer responsable de ello? ¿Al dueño, al fabricante, al diseñador?

Tabla 1. Implicaciones éticas y legales de las nuevas tecnologías

TECNOLOGÍA	ALGUNAS IMPLICACIONES ETICAS Y LEGALES
Inteligencia artificial, Cyborgs, Robots.	Responsabilidad por actividades que generen daños.
Sensores ubicuos, Internet de las cosas.	Problemas relacionados con la protección de datos y la intimidad, al perder el individuo el control sobre su información personal.
Nuevas tecnologías de computación: computación cuántica, procesamiento de redes neuronales.	Nuestro aprendizaje es diferente, perdemos capacidad analítica y concentración.
Tecnologías aplicadas al espacio: microsatélites, telescopios, etc.	Vigilancia excesiva, control "incontrolado".
Realidad aumentada y virtual.	Las cuestiones éticas se refieren a las maneras en las cuales estas tecnologías proveen de nuevas oportunidades para la agencia de las personas, o las restringen; y si son capaces de habituar o desensibilizar a las personas en cuanto a la violencia u otras formas de opresión; incluso, si son capaces de entrenar a las personas en actos antisociales o no éticos.
Tecnologías aplicadas a la energía: Smart grids, etc.	Protección de datos.
Impresión 3D.	Propiedad intelectual e industrial, propiedad de los diseños, etc.

Nanomateriales.	Propiedad intelectual.
Biotecnología.	Consentimiento informado.
Geoingeniería.	Responsabilidad civil.
Blockchain.	Problemas relacionados con la privacidad.

Fuente: elaboración propia a partir de World Economic Forum (2017) Nuevas tecnologías emergentes claves. *The Global Risk Report*.

Un riguroso estudio de los aspectos éticos y sociales con anterioridad al despliegue de la tecnología es la recomendación más razonable[56]. Si los diseñadores son sensibles a ciertos valores éticos que deben integrarse en el mismo diseño, es más fácil anticipar riesgos. Ponemos como ejemplo el trabajo realizado en la Universidad Politécnica de Madrid, la Universidad Autónoma de Madrid y la Universidad de Alcalá de Henares, como un intento de introducir la "privacidad en el diseño" mientras se desarrollaba una tecnología del Internet de las cosas[57]. En el desarrollo de juguetes inteligentes capaces de detectar precozmente dificultades de desarrollo de niños y niñas, los investigadores se esforzaron por atender las recomendaciones de los asesores en privacidad, incluyendo cláusulas de consentimiento informado y estableciendo medidas de seguridad rigurosas que garantizasen en todo momento la privacidad de los menores.

El cambio producido por las Nuevas Tecnologías es más profundo de lo que inicialmente pudiera parecer. Se "re-ontologiza" la realidad, como establece Floridi. El cambio en la Sociedad de la información está transformando nuestra comprensión de la realidad, poniendo retos a las formas convencionales en las cuales hemos estado comprendiendo el mundo y nuestra identidad, en términos de estructuras estables y creencias sólidas.

[56] Wright, D. (2011): "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 13(3), pp. 199–226.

[57] María Luisa Martín-Ruíz, Celia Fernández-Aller, Eloy Portillo, Javier Malagón y Cristina del Barrio (2017): "Developing a System for Processing Health Data of Children Using Digitalized Toys: Ethical and Privacy Concerns for the Internet of Things Paradigm", *Science and Engineering Ethics*.

Construimos nuestra realidad a partir de la información, y de esa forma somos conscientes de nuestros límites. Son precisamente estos los que nos hacen sentirnos humanos. El concepto de "confianza digital" cobra mayor sentido[58].

5.2. Códigos de conducta

Los códigos de conducta constituyen una muestra de autorregulación. En el ámbito de la protección de datos esa capacidad está orientada a la adopción por parte de determinados sectores, de reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por las entidades adheridas, facilitar el ejercicio de los derechos de los afectados, favorecer el cumplimiento de la normativa de protección de datos y demostrar el cumplimiento de dicha normativa.

Característica fundamental de los códigos tipo, derivada de su naturaleza de autorregulación, es el carácter voluntario de la adhesión, siendo vinculantes para las entidades una vez adheridas a los mismos.

De conformidad con lo dispuesto en el artículo 40 del RGPD, las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar aquellos códigos.

Con respecto a los procedimientos de elaboración y adopción el RGPD distingue dos supuestos, los códigos de ámbito exclusivamente nacional (que serán aprobados e incorporados a un registro de códigos de conducta por la AEPD o, en su caso, por la autoridad autonómica de protección de datos competente previa evaluación de su conformidad con el RGPD), y los códigos que afectan a tratamientos en varios Estados de la UE (en cuya tramitación interviene el Consejo Europeo de Protección de datos para la emisión del dictamen sobre su adecuación al RGPD y/o dictamen sobre las garantías ofrecidas para las transferencias internacionales de datos, procediéndose a la suspensión del procedimiento hasta la emisión del informe y, si el dictamen fuera favorable, el Consejo Europeo de Protección de Datos lo presentará a

[58] Education for Information 33 (2017) IOS Press. "New grounds for ontic trust: Information objects and LIS" Betsy Van der Veer Martens School of Library and Information Studies, University of Oklahoma, Tulsa, OK, USA

la Comisión, que decidirá sobre que el código tenga validez dentro de la UE y, en ese caso, le dará publicidad. El Consejo Europeo de Protección de Datos llevará un registro de los códigos de conducta que afecten a tratamientos en varios Estados de la UE y los pondrá a disposición pública).

Los códigos de conducta están regulados en el artículo 38 del PLOPD y pueden ser propuestos prácticamente por cualquier sujeto o entidad que realice un tratamiento de datos, tanto en el sector público como en el privado, por lo que tendrán una relevancia cada vez más significativa en el entorno de la protección de datos.

5.3. Certificación

Uno de los considerandos del RGPD establece expresamente que, para aumentar la transparencia y permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos. Asimismo, se contempla de forma expresa la posibilidad de obtener certificaciones de DPD.

La certificación es voluntaria, es decir, ninguna entidad que trate datos personales está obligada a certificarse, por lo que la certificación es un mecanismo opcional que el RGPD pone a disposición de responsables y encargados con el objeto de facilitar el cumplimiento.

El PLOPD establece, entre las funciones de la AEPD, algunas relacionadas con las certificaciones:

- Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos y aprobar los criterios de certificación.
- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas.

Es importante aclarar que el sólo hecho de que un responsable o encargado disponga de una certificación emitida por un tercero no limita su responsabilidad en cuanto al

cumplimiento, por lo que, ante una irregularidad, la autoridad de control puede ejercer sus funciones y poderes entre los que se encuentra el sancionador.

6. La evolución tecnológica y sus implicaciones: el contexto de la ciberseguridad

La "tecnoética" sugiere la urgencia de una mayor reflexión ética acerca de los retos que presentan las tecnologías emergentes. A partir del análisis ético de este contexto tecnológico cambiante, centraremos las propuestas de cuáles tendrían que ser los derechos digitales irrenunciables que debieran reconocerse en textos vinculantes.

En este contexto, el estudio analizará, entre otros, los retos en el ámbito de la ciberseguridad. Cada vez se cometen mayor número de delitos a través de Internet. Por este motivo, tanto a nivel europeo como español, se han impulsado Estrategias de Ciberseguridad, con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas.

El ciberespacio es hoy algo crucial en la infraestructura de la información y las Comunicaciones. Por ello, la seguridad del ciberespacio se ha transformado en una prioridad de gobiernos y corporaciones. Entendemos el ciberespacio como el mundo electrónico creado por redes interconectadas de tecnologías de la información, en el que más de 1,7 billones de personas están vinculadas para intercambiar ideas, servicios, etc.

Las tecnologías que son ubicuas, interconectadas y permiten acceso fácil a Internet han llegado a estar profundamente integradas en nuestra vida diaria. Como consecuencia de ello, dependemos del ciberespacio para la interacción social, económica y política.

En el ámbito europeo se ha aprobado la Estrategia de Ciberseguridad que establece la estrategia de la UE para prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones en Europa.

Además, el 19 de julio de 2016 se publicó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS (*Network and Information Security*).

En su artículo 1, la Directiva fija su objeto y ámbito de aplicación en los siguientes puntos:

a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

b) crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, "red de CSIRT", por sus siglas en inglés de *computer security incident response teams*) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

e) establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

La Directiva aprobada establece un nivel mínimo de seguridad a las tecnologías, redes y servicios digitales en todos los Estados miembros. También propone establecer la obligatoriedad de que una serie de empresas y organizaciones informen sobre los incidentes cibernéticos de importancia. La lista incluye los motores de búsqueda, los proveedores de servicios en la nube, las redes sociales, las administraciones públicas, las plataformas de pago electrónico, como PayPal, y los principales sitios de comercio electrónico, como Amazon.

La Estrategia de Ciberseguridad y la Directiva sirven de apoyo a la Agenda Digital para Europa, cuyo objetivo es ayudar a los ciudadanos y empresas europeos a aprovechar al máximo las tecnologías digitales. Los actuales sistemas informáticos pueden verse gravemente afectados por incidentes de seguridad, como fallos técnicos y virus. Este tipo de incidentes, a menudo denominados incidentes SRI (los relacionados con la seguridad de las redes y la información) son cada vez más frecuentes y difíciles de atajar.

Numerosas empresas y gobiernos en toda la UE dependen de las redes e infraestructuras digitales para proporcionar sus servicios esenciales. Esto significa que, cuando se produce un incidente SRI, puede tener un gran impacto, pues compromete la prestación de servicios e impide a las empresas funcionar adecuadamente. Además, con el desarrollo del mercado interior de la UE, muchas redes y sistemas de información operan a través de las fronteras. Un incidente SRI en un país puede por tanto afectar a otros o incluso alcanzar a la totalidad de la UE. Los incidentes en materia de seguridad también menoscaban la confianza del consumidor en los sistemas de pago electrónico y en las redes informáticas.

Al adoptar medidas de gestión del riesgo más coherentes y la notificación de incidentes sistemática, la Directiva propuesta ayudará a los sectores que dependen de los sistemas informáticos a ser más fiables y estables.

La estrategia establece una serie de planes para afrontar los desafíos en cinco ámbitos prioritarios:

- Lograr una mayor resistencia cibernética.
- Reducir drásticamente la ciberdelincuencia.
- Impulsar políticas y capacidades en materia de ciberdefensa relacionadas con la política común de seguridad y defensa (PCSD).
- Desarrollar los recursos industriales y tecnológicos en materia de ciberseguridad.
- Establecer una política internacional coherente de la UE sobre el ciberespacio.

En España, lo que se pretende con la Estrategia Española de Ciberseguridad es lograr un uso seguro de los sistemas de información y telecomunicaciones; fortalecer las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques. Muchos son los actores implicados en este asunto: administraciones públicas, Poder Judicial, empresas, ciudadanos, etc., por lo cual, la tarea pendiente es de grandes dimensiones. En concreto, la reforma de la Ley de Enjuiciamiento Criminal por la L.O. 13/2015 introduce medidas gubernativas sin previo mandamiento judicial.

Cada vez se cometen mayor número de delitos a través de Internet (defraudación, pornografía infantil, delitos contra infraestructuras informáticas de las administraciones públicas, entre otros). ¿Será suficiente con las estrategias de ciberseguridad? Muchos retos están abiertos, mientras los gobiernos intentan implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas. Se calcula que, las pérdidas que pueden originarse de no hacer más seguro el ciberespacio rondarían los veinte trillones de euros en 2020.

La Estrategia Española de Ciberseguridad define el ciberespacio, las oportunidades que ofrece y las implicaciones que posee la dependencia de éste, desde el punto de vista de la seguridad. Se detallan y desarrollan ampliamente los principios rectores de la ciberseguridad en España: liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional como extensión de los principios informadores de la Estrategia de Seguridad Nacional. La nueva Estrategia de Seguridad Nacional de 2017[59], que sustituye a la de 2013, aprobada por el Consejo de Ministros (01.12.2017) habla de "ciberamenazas", como amenaza global "que se ha incrementado en número e impacto". Hace referencia al ciberataque de mayo de 2017 *Wanna Cry,* que afectó a empresas y servicios de todo el mundo. En el contexto de la Estrategia de Seguridad Nacional, el Gobierno ha anunciado la creación de un centro

[59] El texto señala que el desarrollo tecnológico "(…) exige una mejor protección de las redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano. España debe adaptarse a esta transformación permanente con un mayor esfuerzo de digitalización y tecnificación del Estado y la sociedad, basado en un sistema educativo y de formación adaptado a la nueva realidad", disponible en http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

de operaciones de seguridad de la Administración del Estado que pretende reforzar la vigilancia y la reacción ante las ciberamenazas. Entre las ciberamenazas que contempla el documento se encuentran los ciberataques y la difusión de noticias falsa o *fake news* en redes sociales e Internet. El centro de operaciones de seguridad será público pero habrá de contar con la colaboración de empresas privadas en régimen de subcontratación.

Podemos resumir los **retos de la ciberseguridad** en estos cuatro:

- Complejidad de un mundo interconectado.

  La evolución del ciberespacio como un mundo electrónico de redes interconectadas, paralelo a nuestro mundo físico, se caracteriza por la enorme cantidad de datos que se almacenan. La economía depende hoy de esta estos datos digitales que se generan a través de transacciones comerciales, comunicaciones, entretenimiento, viajes, tiendas, búsqueda a través de motores de búsqueda, entre otras. Los elementos de estos datos están continuamente siendo combinados, conectados, comparados y vinculados con otra información, dado que las organizaciones intentan capitalizar su valor y ofrecer nuevos servicios de valor añadido a sus usuarios. Los sistemas electrónicos también capturan nuestras preferencias y otros detalles personales, y hacen seguimiento de nuestros movimientos online y cada vez más, offline. El volumen de datos que se genera en el ciberespacio puede incrementarse exponencialmente en cuanto el Internet de las cosas se haga realidad, con sensores que registran localización, estado, actualizaciones en tiempo real y control remoto. El ciberespacio se ha convertido en algo complejo de manejar y con un reto claro de seguridad, en el que la conectividad es permanente a través de móviles, relaciones comerciales a tres bandas, infraestructura de computación en nube, acuerdos que permiten compartir información personal y otros procesos comerciales automatizados.
- Amenazas cada vez más sofisticadas.

  Las amenazas online pueden ser invisibles, pero sus efectos son reales, siendo los sistemas interconectados globalmente accesibles, muy vulnerable. Con el aumento de los flujos de información también se ha producido su aumento de valor para corporaciones, gobiernos y aquellos que poseen malas intenciones.

Nuestros datos dejan ahora una huella digital que nos hace aún más vulnerable a las amenazas.

Donde aparece una oportunidad de negocio, aparece normalmente un mercado para la actividad criminal. Se ha producido una profesionalización del *hacking* malintencionado, con actividades cada vez más sofisticadas. Además, debido a que las empresas raramente reportan las brechas de seguridad, existe información limitada en torno a cómo se llevan a cabo los ataques.

- Las amenazas se mueven cada vez más al mundo móvil.

  En los próximos años, el número de teléfonos móviles habrá excedido el de la población mundial. La cantidad de información que, sobre nosotros, se almacena en nuestros teléfonos, nos hace extremadamente vulnerables ante posibles amenazas de seguridad.

  La Web ofrece una cantidad enorme de servicios que le hacen vital para la nueva economía digital. Al mismo tiempo, las amenazas son cada vez más sofisticadas, y aumentan debido a los siguientes factores: datos cada vez más valiosos que se guardan a gran escala en la nube; máquinas como móviles o *tablets* se integran cada vez más en todas nuestras actividades diarias; la información se comparte y combina con otra con mayor rapidez; Si no conseguimos que todos los componentes del sistema sean seguros, la ciberseguridad no existirá.

  Los países están desarrollando sus Estrategias de Ciberseguridad, que atienden a los sistemas de los gobiernos y también a apoyar a los ciudadanos para conseguir la seguridad online.

  Las amenazas están cada vez más dirigidas a la telefonía móvil, por lo que la protección de datos es crítica. Se utilizan sensores y otros instrumentos que, incluidos en las aplicaciones móviles, permiten hacer seguimiento de lo que las personas descargan, con sus finalidades. Se originan de este modo grandes riesgos, por lo que la industria del móvil, las empresas y los desarrolladores de aplicaciones tienen una gran responsabilidad para velar por la seguridad.

- La paradoja del *big data.*

  Big data puede definirse como el almacenamiento de grandes cantidades de información que se someten a tratamiento y análisis para deducir otras

informaciones. El problema se plantea en cuanto a la implantación de medidas de seguridad que sean efectivas.

Algunos autores han llegado a sugerir, para evitar la necesidad de consentimiento informado (incompatible con la esencia misma de la privacidad), la exigencia de un "interés legítim"[60] como suficiente para facilitar los tratamientos de *big data*. Esto nos parece un asunto muy preocupante, ante el que los expertos en derechos fundamentales no debieran permanecer ajenos.

Al igual que sucede con algunas medidas de seguridad, los esfuerzos por garantizar la ciberseguridad pueden amenazar la privacidad; la relación entre ésta y la ciberseguridad no es armoniosa, debido a que, para conseguir ciberseguridad, se llevan a cabo actividades de monetización y análisis de grandes cantidades de información.

Los tipos de ciberataques contra negocios varían de un sector a otro y están en permanente evolución. Por ejemplo:

- Ha habido un enorme aumento de compañías atacadas a través de fraude al CEO, lo que resulta en pérdidas financieras importantes.
- El sector de los servicios financieros se encuentra como el más directamente atacado.
- Las firmas de servicios profesionales como abogados y auditores están siendo progresivamente más atacados, puesto que sus clientes son grandes corporaciones.
- *Ransomwar*" y *distributed denial-of-service* son ataques que cada vez se usan más contra los negocios de la salud, comunicación social y entretenimiento.
- El sector público y el de las telecomunicaciones son altamente susceptibles de ataques centrados en espionaje.

¿Están nuestras legislaciones y códigos de conducta preparados para afrontar los retos que esto supone?

[60] Moerel, Lokke (2014): *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg University.

7. Recomendaciones y propuestas

La revolución que está suponiendo la digitalización de nuestra economía y nuestra sociedad trae consigo muchos retos en lo que se refiere a conflictos con los derechos de las personas. Tanto las instituciones públicas, como las empresas privadas y los ciudadanos tienen una responsabilidad en cuanto al modo de situarse ante este tema.

Los roles que tradicionalmente han jugado empresas y gobiernos están cambiando, haciendo que las primeras deban incorporar a su cultura la garantía de los derechos y los segundos definir reglas del juego que doten de estabilidad y potencien la transformación digital.

Tal y como hemos venido afirmando en el estudio, la velocidad de los cambios tecnológicos no nos están permitiendo una reacción pausada ante ellos. Los retos que se plantean en relación a los derechos estudiados son muy grandes, mientras que la capacidad de respuesta de la sociedad está muy limitada. Las agendas de los poderes públicos intentan adaptarse a las nuevas situaciones, pero los cambios normativos nunca llegan a tiempo.

Una cuestión que conviene aclarar es que, en general, no se han generado nuevos derechos, los derechos digitales son una extensión de los derechos convencionales. La Declaración Universal de los Derechos Humanos, artículo 12 (intimidad) y artículo 19 (libertad de opinión y de expresión) ofrece una base legal sobre la que continuar trabajando y adaptando las garantías necesarias para su protección.

Teniendo todo esto en cuenta, y con base en todo lo expuesto en los apartados anteriores, formulamos las siguientes recomendaciones y propuestas.

PRIMERA

Una preocupación especial supone el hecho de que una parte de la población se quede relegada frente a las novedades tecnológicas. Nos referimos a la brecha digital en que se encuentra la población más vulnerable, como los más pobres, los mayores,

los niños, las mujeres, que, como es bien sabido, no tienen un papel equiparable al hombre en cuanto al protagonismo en las áreas TIC.

Cada ciudadano hoy en día debe estar capacitado para vivir y trabajar en la sociedad de la información. Para el desarrollo de una sociedad digital se propone una Agenda digital para Europa en los próximos años que promueva entre otros objetivos, el acceso a Internet y su utilización por todos los ciudadanos europeos, especialmente mediante actividades que apoyen la alfabetización digital y la accesibilidad.

Analizar el uso de productos TIC por las personas, en particular el uso del ordenador, el uso de Internet, el uso frecuente de Internet nos proporciona información del perfil de persona que los utiliza, de las diferencias de género en el uso, y del grado de desarrollo de las TIC en la sociedad. Conocer la brecha digital actual entre los usuarios y no usuarios de TIC y más concretamente la que se produce en razón de género contribuye a conocer los factores que la originan: la falta de infraestructura (en particular en las zonas rurales), la falta de conocimientos de informática y habilidades necesarias para participar en la sociedad de la información, o la falta de interés en lo que la sociedad de la información puede ofrecer. El Instituto de Estadística en España sigue admitiendo que existe esta brecha digital de género, en cuanto a la diferencia de uso de las TIC.

Existen variedad de estudios sobre el impacto de la globalización y las TIC sobre el empoderamiento de la mujer[61]. Las conclusiones son muy variadas, en función de los factores que se analicen.

De estas reflexiones, nuestra propuesta iría encaminada a recomendar a todos las instituciones involucradas en la realización de los derechos digitales que se centrasen de forma prioritaria en favorecer a aquella parte de la población que tradicionalmente ha estado relegada en lo que se refiere a los beneficios del avance de la sociedad del conocimiento.

[61] Elia Elisa Cia Alves, Andrea Quirino Steiner (2016): "Globalization, Technology and Female Empowerment: Breaking Rights or Connecting Opportunities?", *Science and Engineering Ethics*.

La mitad de la población mundial no utiliza Internet y, por tanto, no tiene acceso a las oportunidades del mundo digital. Sin embargo, en 2016, aproximadamente el 80% de la población mundial vive en áreas donde la cobertura es de 3G o 4G.

La brecha digital entre países, o entre territorios dentro de un mismo país, crea asimetrías, impide una participación activa y global y aumenta aún más la brecha entre países ricos y pobres. Por eso es necesario un mayor grado de alfabetización digital de las personas, con mayor eficiencia y uso eficaz de los recursos disponibles.

Es necesario, por tanto, romper las barreras económicas, técnicas, sociales y en su caso regulatorias para reducir la desigualdad y la pobreza. Eso significa, por un lado, facilitar el despliegue de las infraestructuras necesarias y, por otro, fomentar la capacitación digital de los ciudadanos. Se trata de una tarea compartida que requiere de un compromiso para alcanzar la plena inclusión de todos en el mundo digital.

SEGUNDA

Muy vinculado con este tema está el de la accesibilidad electrónica, que en este momento supone una obligación sólo para instituciones públicas. No existe en España el mismo nivel de cumplimiento en el ámbito privado, si lo comparamos con el de las administraciones públicas. En este tema hay un reto grande pendiente.

TERCERA

En lo referente a la privacidad, urge que España adapte, según camino iniciado a través del RGPD y PLODP, su legislación a los retos que se plantean en la nueva sociedad digital. Las tecnologías emergentes, como la computación en nube, la Inteligencia artificial, los drones, el *big bata*, traen consigo innumerables retos que hacen muy difícil compatibilizar el derecho a la protección de datos con estos nuevos retos tecnológicos.

El *big data*, por ejemplo, aumenta el riesgo de que las personas pierdan el control sobre sus datos personales. Entre otras cosas, por la enorme escala de la recogida de datos; la seguridad de los mismos, la transparencia –que implica que se dé suficiente información a los titulares de los datos; la posible discriminación, exclusión y

desequilibrio económicos; las posibilidades de mayor vigilancia, tanto por parte de gobiernos, como empresas.

Otro asunto muy relevante es el relacionado con el *social score*, valoración que se hace de cada persona en función de su presencia en las redes sociales. La utilización de este dato es fuente de preocupación, puesto que forma parte del núcleo de la privacidad.

CUARTA

Estrechamente relacionado con la privacidad está el asunto de la seguridad: será importante conocer el estado de los activos tecnológicos y de información de las empresas, así como el modelo de gestión de seguridad de dichos activos, la preparación de las empresas en materia de seguridad TIC, las herramientas y medidas de seguridad que implementan en el desarrollo de su actividad, los incidentes y sus consecuencias desde el punto de vista del negocio y el comportamiento de las empresas en materia de privacidad (protección de datos personales) y transacciones electrónicas.

Según un estudio reciente[62]:

> "Cuanto mayor es la empresa mayor grado de conocimiento muestra de las consecuencias que los incidentes de seguridad pueden tener para su negocio.
> El porcentaje de empresas que declaran haber sufrido algún incidente de seguridad ha aumentado respecto al registrado en 2012. No obstante, lejos de ser un elemento negativo, estas respuestas podrían mostrar cómo ha evolucionado la capacidad de las empresas de identificar la ocurrencia de los distintos incidentes, lo que supondría en consecuencia una mayor capacidad de respuesta.
> Cuantos más activos tecnológicos y de información gestione una empresa y más presencia en Internet haya desarrollado mediante el uso de servicios o la realización de transacciones electrónicas, la empresa indica que aborda más riesgos e incidentes de seguridad. La creciente declaración sobre el uso de activos y servicios electrónicos parece indicar que las empresas se exponen a crecientes problemas de seguridad, por lo que en un entorno como el actual, la seguridad TIC de la empresa se convierte en un elemento esencial para la estabilidad del negocio de las empresas.

[62] ONTSI (2017a: 7).

> Al contrario de lo que cabría esperar, las empresas que tienen definida una política de seguridad también sufren más incidentes de seguridad, lo que probablemente tiene que ver con la existencia de registros específicos que permiten su gestión, una mayor capacidad de aminorar sus consecuencias y una mayor consciencia de la ocurrencia concreta de los incidentes.
> Se puede concluir que la existencia de una política de seguridad no disminuye necesariamente la existencia de incidentes, sino que permite una adecuada gestión de los mismos, aminorando su impacto.
> Las grandes empresas mencionan que sufren un menor número de consecuencias negativas derivadas de incidentes de seguridad. De esta forma, el hecho de que las grandes empresas sufran mayor número de incidentes de seguridad y, por el contrario, denoten menores consecuencias, refuerza la idea de que su mayor preparación ante los incidentes minimiza las consecuencias negativas que estos tienen para su negocio.
> Se ha detectado un bajo porcentaje de empresas que declaran haber cuantificado el impacto económico que han tenido los incidentes de seguridad. Esta sin duda parece una tarea pendiente para el futuro.
> Al contrario de lo que cabría imaginar, existe una relación inversamente proporcional entre el tamaño de las empresas y la cuantificación del impacto económico producido por los incidentes de seguridad, así, las microempresas son las que declaran haber cuantificado los daños económicos en un mayor porcentaje, 44%, seguidas de las pequeñas empresas con un 31%, medianas empresas 29% y, finalmente, grandes empresas 27%.
> El cambio de hábitos como consecuencia de haber sufrido un incidente de seguridad presenta diferencias según el tamaño de la empresa, de manera que: las microempresas y pequeñas empresas han manifestado en mayor proporción dejar de usar determinados servicios de Internet y haber comenzado a realizar copias de seguridad, mientras las medianas y grandes empresas indican en mayor medida que establecen protocolos y procedimientos de seguridad más estrictos, o bien contratan servicios de auditoría externos."

Otra línea de trabajo importante es el trabajo de las instituciones públicas con la industria para conseguir la creación de un medio ambiente digital seguro para todos los usuarios/as, en el que las empresas que piensen primero en este asunto de la seguridad sobre cualquier otro[63]. Preocupa especialmente el mundo de las redes sociales, el marketing online y los juegos por Internet.

[63] UK Government (2017: 21).

En general, todas las propuestas deben partir de los siguientes principios:

- Lo que es inaceptable en el mundo analógico, también debe serlo en el mundo online.
- Todos los usuarios y usuarias deben estar empoderados para manejar los riesgos online y permanecer seguros.
- Las empresas tecnológicas tienen una responsabilidad con respecto a sus usuarios. Es urgente que aprueben políticas centradas en su compromiso con los derechos digitales: privacidad, seguridad, neutralidad en la Red, brecha digital, entre otros. En este sentido, el RGPD presenta una oportunidad con los principios de "privacidad en el diseño" y los estudios de impacto en la privacidad.

Nos parece especialmente relevante este último tema. Aunque el RGPD no obliga a llevar a cabo estos estudios en todo caso, creemos que una utilización extendida de los estudios de impacto en la privacidad puede ayudar a crear una cultura de respeto a la protección de datos en las instituciones. Estos estudios debieran contener como elementos esenciales los siguientes: (1) disponibilidad de la información personal, (2) integridad, (3) confidencialidad, (4) imposibilidad de vincular o cruzar información personal, (5) transparencia, (6) control del titular y el responsable sobre los datos personales.

QUINTA

En relación a la desconexión laboral, se propone:

- Regular el derecho a la desconexión digital laboral en los convenios laborales y en el ET, como un derecho. Si por razones de disponibilidad laboral, productividad u otras razones el trabajador debe estar disponible digitalmente, ha de quedar estipulado o en el convenio colectivo o en el contrato de trabajo, con el fin de poder regular de la manera más racional posible sus tiempo laboral efectivo.
- Formación e información al trabajador sobre su derecho a no mantener comunicación por motivos laborales más allá de la jornada de trabajo, sabiendo que todas las horas que excedan de la jornada establecida computarían como horas extraordinarias. La dificultad de conocer el tiempo

efectivo de trabajo a través de medios digitales puede dificultar el cómputo. Para conocerlo con exactitud se pueden implantar instrumentos técnicos por parte de la empresa.

- Limitar los mecanismos de comunicación digital entre el trabajador y su empresa a través del correo, aplicaciones móviles, móvil, etc., de manera que queden garantizados el tiempo efectivo de jornada laboral y el de descanso. El contenido del derecho comprendería el derecho a no recibir correos electrónicos tras la jornada laboral y el derecho a no conectarse a Internet para cuestiones laborales, por medio de *tablets*, *smartphones*, información en la nube, etc.

SEXTA

Otro asunto que merece especial atención es el de la neutralidad de la Red. A pesar de estar regulado, el control de las previsiones legales está lejos de llevarse a cabo de manera efectiva. Y por otro lado, gran parte de la ciudadanía permanece ajena a este asunto, ignorando la relevancia que tiene sobre sus derechos. Se propone un mayor compromiso proactivo de los proveedores de servicios de acceso a Internet para tratar todo el tráfico a través de la Red de manera equitativa.

SÉPTIMA

Otro asunto clave que merece reflexión es el de la necesidad o no de una "Constitución Digital". Nos remitimos a las reflexiones del Prefacio de este estudio sobre la conveniencia de una "Declaración de Derechos y Obligaciones en el Entorno Digital", de naturaleza política, en un ámbito español, europeo o más allá, si fuera posible, alentado por el G-20. Esta declaración política podría impulsar una declaración con fuerza jurídica en aquellos países que lo asumieran o en una dimensión transnacional.

OCTAVA

En cuanto a la educación, es necesario transformar los modelos educativos, los procesos de aprendizaje y la enseñanza mediante la adopción de tecnologías digitales y servicios basados en recursos y estándares abiertos. Así mismo, es necesario desarrollar modelos de Innovación Abierta y Estándares Abiertos, evitando

medidas injustificadas para proteger la propiedad intelectual que puedan obstaculizar los procesos de innovación en la Economía Digital.

Se propone:

- Favorecer la educación digital de los ciudadanos, en los diferentes niveles educativos, incorporando materias con contenidos que permitan a los alumnos/as adquirir las capacidades y habilidades necesarias para la utilización adecuada y útil de Internet.
- Favorecer el acceso a los contenidos educativos universal y gratuito, o con tarifas razonables, y debe garantizarse la igualdad de oportunidades, sin que pueda provocarse una brecha digital. Aprovechar las ventajas de Internet para impartir los conocimientos educativos de las materias que así lo permitan (que todas lo permiten). Para llevar a cabo esta acción será necesario implantar los instrumentos técnicos y tecnológicos de una manera racional y sin discriminación entre centros urbanos y rurales, así como entre centros públicos y concertados. Por tanto, habrá que realizar un esfuerzo de medios materiales y económicos por parte de las Administraciones implicadas, pero también una aportación generosa, responsable y comprometida de las empresas que oferten dichos servicios, con el fin de promover la extensión de los servicios a todos los ciudadanos en los centros escolares.

NOVENA

En el ámbito de la organización política, se están alterando los modelos tradicionales de relación y organización de las sociedades contemporáneas. Cuestiones esenciales que van desde la seguridad nacional a la salud pública, se ven afectadas por el desarrollo de la tecnología, y la división entre lo público y lo privado es cada vez más difusa.

El nuevo escenario exige que la concepción territorial del poder se adapte a una "sociedad hiperconectada" y abierta, en la que conceptos como la transparencia, la gobernanza, la participación y la rendición de cuentas se convierten en imprescindibles si queremos seguir contando con democracias fuertes.

Es urgente mantener la confianza en las instituciones y valores democráticos para garantizar el buen funcionamiento del Estado de derecho y la aplicación efectiva de los derechos humanos en un nuevo contexto caracterizado por la irrupción y el protagonismo de la innovación tecnológica. Desde la relación de las administraciones públicas con los ciudadanos, hasta las empresas con sus clientes, o los actores de la sociedad civil, todos debemos asumir nuevos roles y responsabilidades.

DÉCIMA

Existe una propuesta para poner en marcha de la denominada Quinta Generación de la Historia de los Derechos Fundamentales, los derechos 5G. Creemos que, aunque hay que reforzar algunos derechos (a la privacidad, especialmente), y crear algún otro (a la neutralidad de la Red, a la desconexión laboral, entre otros), los problemas y retos que se plantean no van a ser solucionados a través de nuevas legislaciones, menos si éstas son internacionales. La normativa internacional no es fácilmente exigible, y nada de lo que se regule así tendrá aplicabilidad real en el corto plazo.

Por ello, creemos que el reto no radica en nuevas legislaciones (salvo asuntos muy concretos), sino en un cambio en las políticas de las instituciones, públicas y privadas, además de en la sensibilización de la ciudadanía hacia un mayor respeto hacia la dignidad de los demás, evitando conductas centradas en el "aprovechamiento ilícito" de los contenidos digitales[64], por ejemplo.

DECIMOPRIMERA

Los ciudadanos pierden, en ocasiones, la confianza en el mundo digital. A veces, el exceso de información les deja con una sensación de saturación y desinformación. Sus datos personales se tratan por parte de muchos actores, pero no son informados suficientemente de ello. Algunas otras propuestas para reaccionar contra los daños a los derechos que se producen en el mundo virtual serían:

- Adaptar la legislación, endureciendo las penas por violación de la ley.
- Respuesta rápida de las policías a los crímenes online
- Estrategias gubernamentales coordinadas
- Especial atención al fraude a población vulnerable, como mayores y menores.

[64] ONTSI (2017b).

- Hacer realidad la portabilidad de la vida digital para que los consumidores puedan usar sus datos, información y aplicaciones de forma independiente al dispositivo o plataforma en uso.
- Promover la interoperabilidad de aplicaciones de Internet y servicios de comunicación y mensajería para mejorar la experiencia del usuario y favorecer la competencia.
- Incrementemos la transparencia de las condiciones de uso de los servicios de Internet y la diferenciación entre publicidad e información en los resultados de las búsquedas online.

DECIMOSEGUNDA

Los retos que plantea la digitalización de nuestra sociedad no son fácilmente asumibles por un actor de forma aislada. Proponemos la alianza de actores de diversa naturaleza (al modo de las Alianzas Público-Privadas, por ejemplo) y el trabajo en red, de forma que puedan abordarse los retos complejos que se plantean.

Referencias bibliográficas

1. Andrews, L. (2011): *Social Networks and the death of privacy. I know who you are and I saw what you did,* Free Press.
2. BBVA (2016): *El próximo paso: la vida exponencial.*
3. Cantijoch, M. (2014): *La desigualdad digital, ¿una nueva fuente de desigualdad política?,* Fundación Alternativas.
4. Cannataci, Joseph A. (2016): *Informes del Relator de Naciones Unidas para el derecho a la privacidad,* A/HRC/31/64.
5. Castells, M. (2000): "The Information Age: Economy, Society and Culture", *Volume I: The Rise of the Network Society,* Oxford: Blackwell.
6. Clarke, S. (2010): "On New Technologies", en L. Floridi (ed.): *The Cambridge Handbook of Information and Computer Ethics,* Cambridge: Cambridge University Press, 234-248.
7. Comisión Europea (2014): Comprender las políticas de la Unión Europea: Agenda Digital para Europa, Luxemburgo: Oficina de Publicaciones de la Unión Europea, p. 3 (https://europa.eu/european-union/file/1501/download_es?token=3l7D0Fil).
8. De Hert, Paul, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay y Ignacio Sanchez (2017): "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer law & Security Review*.
9. Fernández Burgueño, Pablo (2012): "Aspectos jurídicos de la identidad digital y la de la Comunicación", *adComunica, Revista de Estrategias, Tendencias e Innovación en Comunicación,* nº 3.
10. Floridi, L. (2013): *The ethics of information society in a globalized world*, Oxford University Press.
11. Floridi, L. (ed.) (2010): *The Cambridge Handbook of Information and Computer Ethics*.
12. García Mexia (2017): *La Internet abierta. Retos regulatorios de una Red nacida libre,* RDU Ediciones.

13. Goig Martínez, J.M., Núñez Martínez, M.A., Núñez Rivero, C. (2006): *El sistema constitucional de derechos y libertades según la Jurisprudencia del Tribunal Constitucional*, Ed. Universitas Internacional, p. 274.
14. Guichot, E. (2011): *Transparencia y acceso a la información pública en España: análisis y propuestas legislativas*, Fundación Alternativas, Documento de trabajo 170/2011.
15. Johnson, D. G. (1997): "Is the Global Information Infrastructure a Democratic Technology?", *Computers and Society* 27, 20–26.
16. Johnson, D. G. (1985): *Computer Ethics*, Englewood Cliffs, NJ: Prentice Hall.
17. KPMG (2017): *Closing the gap. Insuring your business against evolving cyber threats*.
18. Lanier, J. (2014): "Nuevas concepciones de la privacidad", *Investigación y Ciencia*, nº 448.
19. Levmore y Nussbaum (2010): *The offensive Internet*, Harvard University Press.
20. López Garrido, D., Massó Garrote. M., y Pegoraro, L., (directores) (2017): *Derecho Constitucional Comparado*, Tirant lo Blanch, Valencia.
21. López Garrido, D. (1989): *La crisis de las telecomunicaciones. El fenómeno desregulador en Estados Unidos, Japón y Europa*, Fundesco, Madrid.
22. Manyika J., Chui M., Bughin J., Dobbs R., Bisson P. y Marrs A. (2013): *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey & Company.
23. Ministerio de Hacienda y Administraciones Públicas (2012): *Guía de comunicación digital para la Administración General del Estado* (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Guia_de_Comunicacion_Digital_para_la_Administracion_General_del_Estado.html#.Wjvu89ThBaY)
24. OECD (2017) *Digital Economy Outlook.*
25. ONTSI (2017a) *Encuesta sobre confianza digital en las empresas*.
26. ONTSI (2017b) *El Estudio de Uso y Actitudes de Consumo de Contenidos Digitales.*

27. Pérez Tornero, J.M. (2005): "El futuro de la sociedad digital y los nuevos valores de la educación en medios", *Comunicar: Revista científica iberoamericana de comunicación y educación,* 25-1, pp. 247-258.
28. Rebollo Delgado, L. y Serrano Pérez, M. M. (2014): *Manual de protección de datos*, Dykinson.
29. Rebollo Delgado, L. y Serrano Pérez, M. M. (2006/2008): *Introducción a la protección de datos*, Dykinson, 1ª y 2ª ED., Madrid.
30. Royal Society and the Royal Academy of Engineering (2004): "Nanoscience and Nanotechnologies: Opportunities and Uncertainties" (www.nanotec.org. uk/finalReport).
31. Serrano Pérez M. M. (2017): "La garantía de la protección de datos personales y del trato de los pacientes que no sean ciudadanos del Estado español", en Cantero, J. (dir.): *La Liberalización de la Asistencia Sanitaria Transfronteriza en Europa*.
32. Serrano Pérez M. M. (2015): "Los principios del buen gobierno del art. 26 de la Ley 19/2013, de 9 de diciembre de transparencia, acceso a la información y buen gobierno", en Troncoso Reigada, A.: *Comentarios a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno*, Thomson.
33. Serrano Pérez M. M. (2015): "Big Data o la acumulación masiva de datos sanitarios: derechos en riesgo en el marco de la sociedad digital", *Derecho y Salud*, vol. 25.
34. Serrano Pérez M. M., Navarro, C. y Zurriaga, Ó. (2013): "A modo de reflexión y crítica en torno a la propuesta de Reglamento europeo de protección de datos de carácter personal y algunas enmiendas presentadas en relación con la epidemiología y la salud", *Derecho y Salud*, vol. 23.
35. Serrano Pérez M. M. (2013): "Salud pública, epidemiología y protección de datos", en Palomar Olmeda A., Cantero Martínez J.: *Tratado de Derecho Sanitario,* Vol. II, Thomson Reuters-Aranzadi, Cizur Menor (Navarra).
36. Serrano Pérez M. M. (2013) "Los derechos al honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos", en García Guerrero, J. L. (dir.): *Los derechos fundamentales,* Tirant lo Blanch, Valencia.

37. Serrano Pérez M. M. (2010): “Los derechos de rectificación y cancelación”, en Troncoso Reigada, A.: *Comentario a la Ley Orgánica de protección de datos de carácter personal,* Thomson-Reuters.
38. Serrano Pérez M. M. (2003): *El derecho fundamental a la protección de datos en Derecho español y comparado,* Thomson-Cívitas, Madrid.
39. Steck C., Moreno N., López-Barajas G., Seriñá J., Villa P., Vida A.l, Serra E., Bartholomew S. y Shipp J. (2014): *Manifiesto Digital. Por una Internet abierta y segura para todos,* Telefónica.
40. UK Government (2017): *Internet Safety Strategy – Green paper.*
41. Van den Hoven, J. (2008): “Moral Methodology and Information Technology”, en Himma, K. E. and Tavani, H. T. (eds.): *The Handbook of Information and Computer Ethics*, pp. 49–69.
42. Van der Veer Martens, B. (2017): “New grounds for ontic trust: Information objects and LIS”, *Education for Information*.

Anexos

A.1. Legislación

- Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). Esta norma tiene su fecha de derogación ya señalada pues se ha aprobado el Reglamento de Protección de Datos que entrará en vigor en mayo de 2018 y que será directamente aplicable en las cuestiones que el Reglamento regule al detalle; no obstante el proyecto de Ley de protección de datos ya ha empezado a elaborarse, para las cuestiones que la norma europea deja a criterio de los Estados miembros, así como para clarificar parte del articulado.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE).
- Ley Orgánica 2/2006, de 3 de mayo del Educación (LOE).
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT), en respuesta a los cambios en materia de telecomunicaciones regulados por la Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Derechos de los Usuarios), y la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (BOE núm. 97, de 22 de abril de 1996) (LPI); La Ley de propiedad intelectual ha sido objeto de reformas a través de la Ley 23/2006, de 7 de julio y por la Ley 21/2014, de 4 de noviembre, en ambos casos por las que se modifica el texto refundido de la Ley de Propiedad Intelectual.

- Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Directiva (UE) 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
- Directiva (UE) 2016/2102 del Parlamento y del Consejo de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.
- Reglamento (UE) 2015/2120, de 25 de noviembre de 2015, del Parlamento Europeo y del Consejo, por el que se establecen medidas en relación con el acceso a un Internet abierto y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión, DOUE L 310, de 26 de noviembre de 2015.
- 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).
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS.

A.2. Glosario de términos

Dentro de la sociedad digital debemos empezar a delimitar un conjunto de términos específicos que por su carácter técnico han de ser definidos:

- **Accesibilidad electrónica**

  El derecho de acceso a las TIC en condiciones de igualdad, con independencia de la discapacidad. Se trata del acceso y utilización de tecnologías, productos y servicios relacionados con los servicios de la sociedad de la información y de cualquier medio de comunicación social.

- **Administración electrónica**

  Modo de relacionarse los ciudadanos con la Administración a través de las TIC.

- **Anonimización**

  En el proceso de anonimización se deberá producir la ruptura de la cadena de identificación de las personas

  La finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

- **Brecha digital**

  Diferencia en el acceso, uso y aprovechamiento de las TIC.

- ***Big Data***

  Término utilizado para definir la gestión de información de manera masiva. Herramienta que permite la gestión y análisis de enormes volúmenes de datos de forma no convencional.

- ***Block chain***

  Base de datos distribuida que consiste en cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado.

- **Ciberseguridad**

  La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y

todo lo relacionado con ésta, especialmente, la información contenida en un ordenador o en redes de ordenadores, Internet, etc.

- **Código abierto**

  Open source o código abierto consiste en un software distribuido bajo una licencia que permite al usuario acceso al código fuente. Este tipo de licencia posibilita el estudio y la modificación del software con total libertad. Además, su redistribución está permitida siempre y cuando esta posibilidad vaya en concordancia con los términos de licencia bajo la que se adquiere el software.

- **Comercio electrónico**

  Concepto que se refiere a hacer negocios electrónicamente. Incluye todas las etapas de la transacción así como todos los servicios de las mismas y las relaciones entre empresas.

- **Confianza digital**

  Es aquella que permite construir un clima que contribuya al desarrollo de la economía y la sociedad digital, disponer de un ciberespacio abierto, seguro y protegido, garantizar un uso seguro de las redes y los sistemas de información, y responder además a los compromisos internacionales en materia de ciberseguridad.

- **Datos de carácter personal**

  Cualquier información concerniente a personas físicas identificadas o identificables.

- **Delegado de protección de datos**

  Esta figura, conocida popularmente como DPO (en inglés, Data Protection Officer), es uno de los elementos claves del RGPD, y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control. Es decir, al Delegado de Protección de Datos, que deberá contar con conocimientos especializados del Derecho, y obviamente en protección de datos, que actuará de forma independiente, se le atribuyen una serie de funciones reguladas en el artículo 39 del RGPD, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado.

- **Democracia electrónica**

  La forma en la que las TIC contribuyen a otorgar poder a la ciudadanía y a hacerla más partícipe en los procesos de decisión política, mejorando la comunicación y la proximidad entre los representantes políticos y los ciudadanos.

- **Evaluación de impacto en la protección de datos personales**

  Consiste en un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados. Tras ese análisis, se debe afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

- **Inclusión digital**

  Utilización de la tecnología para favorecer la adquisición de competencias de alumnos/as con necesidades educativas especiales.

- **Inteligencia artificial**

  Simulación de procesos de inteligencia humana por parte de máquinas, especialmente sistemas informáticos. Estos procesos incluyen el aprendizaje (la adquisición de información y reglas para el uso de la información), el razonamiento (usando las reglas para llegar a conclusiones aproximadas o definitivas) y la autocorrección.

- **Neutralidad en la Red**

  Principio en virtud del que cualquier persona ha de tener acceso a los contenidos de Internet en igualdad de condiciones.

- **Privacidad desde el diseño**

  Consiste en la visión de que el futuro de la privacidad no puede ser garantizada solo por cumplir con los marcos regulatorios; más bien, la garantía de la privacidad debe convertirse en el modo de operación predeterminado de una organización. Privacidad por Diseño se extiende a una "Trilogía" de aplicaciones que engloban: 1) sistemas de tecnologías de la información; 2) prácticas de negocio responsables; y 3) diseño físico e infraestructura en red.

- **Pobreza tecnológica**

  Nueva manera de entender la pobreza que tiene en cuenta la dificultad en el acceso a las TIC, lo cual trae consigo la profundización en la situación de desventaja económica y en las posibilidades de desarrollo humano.

- **Portabilidad**

  Consiste en la posibilidad de obtener, "en un formato electrónico estructurado y comúnmente utilizado", una copia de los datos que están siendo objeto de tratamiento, formato que debe permitir que puedan seguir siendo utilizados por la persona interesada (se entiende que en otro sistema o aplicación informática).

  Además, consiste en la posibilidad de optar por transmitir esos datos a otro sistema (a otro proveedor o prestador de servicios), siempre que los datos sobre los que se pretenda llevar a cabo la trasmisión estén sometidos a tratamiento automatizado, para lo que también se prevé que estos sean transmitidos en un "formato electrónico comúnmente utilizado", todo ello sin que el responsable del tratamiento ponga trabas, impedimentos o dificultades para la retirada de esos datos.

- ***Smart Grids***

  Red eléctrica inteligente que puede automatizar y manejar la creciente complejidad y necesidades de electricidad del siglo XXI, eficiente, segura y capaz de responder de forma inmediata ante cualquier corte de suministro.

- **Sociedad digital**

  Aquella sociedad en la que se ha producido una transformación digital, debido al uso masivo de las TIC.

- **Tecnologías de la información y las Comunicaciones (TIC)**

  Las TIC se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de hardware y software

Siglas y abreviaturas

ACM	Association for Computer Machinery
AEPD	Agencia Española de Protección de Datos
ASU	Acceso y Servicio Universal
AU	Acceso Universal
CEDH	Convención Europea de Derechos Humanos
CSIRT	Computer Security Incident Response Team
DOUE	Diario Oficial de la Unión Europea
GT29	Grupo de Trabajo del Artículo 29
IDI	Índice de Desarrollo de las TIC
IEEE	Institute of Electric and Electronic Engineering
ITU	International Telecommunications Union
LODE	Ley Orgánica de Educación
LOPD	Ley Orgánica de Protección de Datos
LSSICE	Ley de Servicios de la Sociedad de la Información y Comercio Electrónico
NIS	Network Information Security
NSA	National Security Agency
OECD	Organización para la Cooperación y el Desarrollo Económicos
OSCE	Organización para la Seguridad y la Cooperación en Europa (OSCE)
PCSD	Política Común de Seguridad y Defensa
PLOPD	Proyecto de Ley Orgánica de Protección de Datos
RD	Real Decreto
RFID	Identificación por Radio Frecuencia
RGPD	Reglamento General de Protección de Datos
SRI	Seguridad de Redes e Información
STC	Sentencia del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
SU	Servicio Universal
TEDH	Tribunal Europeo de Derechos Humanos

TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea
UNE	Una Norma Española
WAI Web	Accessibility Initiative

Últimos Documentos de Trabajo publicados

194/2016. **Prescripción enfermera: situación actual, problemas y alternativas. M**aría Luisa Fernández Ruiz

193/2016. **Las reformas económicas del futuro: un nuevo modelo de crecimiento para España.** Ramon Xifré y Jordi Salvador

192/2016. **Informe sobre la Transparencia Corporativa en España: una visión desde el sector empresarial, los medios de comunicación y las organizaciones pro-transparencia.** Elena Mañas y Óscar Montes

191/2016. **¿Ha podido más la crisis o la convivencia? Sobre las actitudes de los españoles ante la inmigración.** Héctor Cebolla Boado y Amparo González Ferrer

190/2015. **Análisis y propuestas para la regeneración de la sanidad pública en España.** Javier Rey del Castillo

189/2014. **La internacionalización en la base de la pirámide empresarial española: análisis y propuestas.**Ramon Xifré Oliva

188/2014. **El impacto de la crisis sobre el tejido social solidario de España: efectos y reacción de las ONGD frente a la crisis.** Kattya Cascante y Érika Rodríguez

187/2014. **El modelo territorial español treinta y cinco años después.** Tomás de la Quadra Salcedo

186/2014. **El derecho al olvido digital.** Luis Javier Mieres Mieres.

185/2014. **Los parados de larga duración en España en la crisis actual.** Sara de la Rica y Brindusa Anghel.

184/2014. **Medidas sociales para combatir el fraude fiscal en España.** María Goenaga Ruiz de Zuazu.

183/2014. **El copago sanitario: resultados para el sistema sanitario y los pacientes.** Manuel Martín García.

182/2014. **La privatización de la asistencia sanitaria en España.** Marciano Sánchez Bayle.

181/2013. **Gestión pública del hecho religioso en España.** José M.ª Contreras Mazarío.

180/2013. **Identidad social, pluralismo religioso y laicidad del Estado.** Ana Fernández-Coronado y Gustavo Suárez Pertierra.

179/2013. **El uso de símbolos religiosos en el espacio público en el Estado laico español.** Fernando Amérigo y Daniel Pelayo.

178/2012. **Los ciudadanos españoles ante la crisis.** Olga Salido.

177/2012. **La Economía Social y la atención a la dependencia. Propuestas para contribuir al desarrollo de los servicios de atención de la dependencia y a la generación de empleo estable y de calidad.** Antonio Jiménez Lara y Ángel Rodríguez Castedo.

176/2012. **La integración de las energías renovables en el sistema eléctrico.** Alberto Carbajo Josa.

175/2011. **Los sindicatos españoles: voz e influencia en las empresas.** Carmen García-Olaverri y Emilio Huerta.

174/2011. **Gestión de listas de espera en el Sistema Nacional de Salud. Una breve aproximación a su análisis.** Agustín Cañizares Ruiz y Álvaro Santos Gómez.

173/2011. **Una nueva Ley General de Sanidad para sostener el Sistema Nacional de Salud.** Javier Rey del Castillo.