UNA NUEVA GENERACIÓN DE DERECHOS DIGITALES[1]

A new generation of digital rights

ARTEMI RALLO LOMBARTE
Universidad Jaume I de Castellón
rallo@uji.es

Cómo citar/Citation
Rallo Lombarte, A. (2020).
Una nueva generación de derechos digitales.
Revista de Estudios Políticos, 187, 101-135.
doi: https://doi.org/10.18042/cepc/rep.187.04

Resumen

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales da respuesta a la necesidad de garantizar en la sociedad digital contemporánea derechos que garanticen la subordinación de la tecnología al individuo y que preserven su dignidad en la totalidad de ámbitos en que las personas actúan en sociedad. Los nuevos derechos digitales incluidos en su título X son el corolario de la evolución protagonizada por la sociedad contemporánea, pero esta elevación a rango legal de un catálogo de derechos digitales plantea numerosos interrogantes y reflexiones sobre su base constitucional, su colisión con otros derechos y libertades, su garantía efectiva y su desarrollo futuro. Este trabajo demuestra que garantizar derechos digitales no implica únicamente procurar que los ciudadanos no vean limitada su capacidad de uso de la tecnología o preservar que los individuos puedan hacer valer sus derechos frente a la tecnología. La garantía efectiva de los derechos en la era digital impone obligaciones a los poderes públicos para posibilitar un acceso pleno a las herramientas tecnológicas que permita el desarrollo de su personalidad en el mundo contemporáneo en tanto realidad digital.

[1] Una versión preliminar de este trabajo, realizada desde el análisis del impacto evolutivo del derecho de protección de datos, ha sido publicada en Rallo Lombarte (2019a).

Palabras clave

Internet; derechos digitales; protección de datos; tecnología; privacidad; derecho al olvido; videovigilancia; derechos humanos.

Abstract

The Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights, provides an answer to the need to guarantee, in the contemporary society, rights to subordinate technology and to preserve dignity and individual rights in all social areas. But new digital rights included in Title X raise several questions on its constitutional basis, its collision with other rights and freedoms, its effective guarantee and its future development. This paper shows that guaranteeing digital rights does not imply only ensuring that citizens do not see limited their ability to use technology or that individuals can enforce their rights in the face of technology. The effective guarantee of rights in the digital age imposes obligations on the public authorities to enable full access to the technological tools that allow developing human personality in the contemporary digital world.

Keywords

Internet; digital rights; data protection; technology; privacy; right to be forgotten; videosurveillance; human rights.

SUMARIO

I. INTRODUCCIÓN

«Tenemos que situarnos en el futuro […] vendrán otras muchas técnicas —no solo la informática—, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera […]. Hay que evitar la traición de la tecnología; hay que arbitrar nuevos sistemas de valores»[2]. Cuatro décadas después de pronunciarse estas premonitorias palabras, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante, LOPDGDD) supone la respuesta actual a las angustiosas reflexiones efectuadas durante los debates constituyentes en tanto manifestación paradigmática de la transformación provocada por la tecnología en la sociedad actual. La sociedad digital demanda un haz de derechos que garanticen la subordinación de la tecnología al individuo, preserven su dignidad y se proyecten sobre la totalidad de los ámbitos en que actúa en sociedad. Los nuevos derechos digitales incluidos en el título X son el corolario de la evolución protagonizada por la sociedad contemporánea durante las últimas décadas[3].

[2] *Constitución española. Trabajos parlamentarios*, Tomo I, Madrid, Cortes Generales, 1980, pp. 1068 y ss. Estas visionarias palabras de Isaías Zarazaga, senador constituyente, advertían en 1978 de la era de cambios a los que la tecnología emergente sometería a la sociedad.

[3] Este título X ("Garantía de los derechos digitales") fue introducido durante el *iter* legislativo a raíz de una enmienda presentada por el Grupo Parlamentario Socialista *(Boletín Oficial de las Cortes Generales. Congreso de los Diputados*, núm. A-13-2, de 18 de abril de 2018).

Ahora bien, la elevación a rango legal de un catálogo de derechos digitales invita a formular una serie de interrogantes y reflexiones sobre su base constitucional, su colisión con otros derechos y libertades, su garantía efectiva y su desarrollo futuro (Pérez Luño, 2012). Los derechos digitales adquieren una dimensión multifacética que residencia tanto en el individuo —en un doble plano activo y pasivo— como en los poderes públicos su garantía efectiva. Garantizar derechos digitales no implica únicamente procurar que los ciudadanos no vean coartada o limitada su capacidad de uso de la tecnología o preservar que los individuos puedan reaccionar haciendo valer sus derechos frente a la tecnología.

Algunos de estos derechos limitan su alcance a una dimensión geográfica concreta, lo que posibilita su operatividad y garantía efectiva. Otros derechos, sin embargo, adquieren una dimensión global, pues se proyectan plenamente en el espacio virtual construido sobre la existencia de internet (García Mexía, 2005, 2009; Barrio Andrés, 2017a) cuyo impacto no admite matices (Rallo Lombarte y Martínez, 2013b; Davara Fernández de Marcos, 2016). Así lo proclama el preámbulo de la LO 3/2018: «internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad»[4]. Los interrogantes que suscita esta compleja realidad no serán fáciles de resolver, pero este trabajo pretende contribuir a ello.

II. LA LEY LIMITARÁ EL USO DE LA INFORMÁTICA PARA GARANTIZAR EL PLENO EJERCICIO DE LOS DERECHOS DE LOS CIUDADANOS

Como ya hemos tenido ocasión de afirmar recientemente (Rallo Lombarte, 2017a: 637-667, 2018a: 2363-2379), la referencia a *la informática* en el texto constitucional de 1978 resulta altamente meritoria por vanguardista y por otorgar trascendencia constitucional a la necesidad de proteger al individuo frente a los primeros avances tecnológicos («la informática») y ante los riegos que se cernían en el disfrute de derechos fundamentales: «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 CE).

[4] El preámbulo de la *Dichiarazione dei diritti in Internet,* aprobada el 28 de julio de 2015 por la Camara de Diputados italiana, se expresa en similares términos.

Este precepto sitúa a la Constitución española en la vanguardia de las normas fundamentales de su tiempo, pues pretende adecuar la normativa constitucional a nuevas realidades sociales que ya afectaban al ser humano en su dignidad y derechos y que, premonitoriamente, podrían incidir en el futuro en esta esfera individual (Troncoso Reigada, 2010).

Aparentemente, el tenor literal del art. 18.4 CE ofrece una inequívoca e incuestionable justificación (más bien un mandato) constitucional para que el legislador futuro garantice la totalidad de los derechos de los individuos (particularmente, algunos de ellos como el honor e intimidad por su singular afectación) frente al uso de la informática (término que reconduce a la tradicional «automatización» pero que la realidad actual referiría a la «tecnología digital»). Pero, durante décadas, la esfera aplicativa de este precepto ha quedado circunscrita, como veremos, al ámbito de la protección de datos personales. No en vano, las distintas leyes de protección de datos que ha conocido nuestro país (LORTAD, LOPD y LOPDGDD) han sido calificadas siempre como las normas de desarrollo de este precepto constitucional con una apariencia de exclusividad excluyente. En otras palabras, como si en el ámbito de protección de este precepto únicamente cupiese la garantía del derecho de protección de datos. ¿Es esto así o, más bien al contrario, estamos ante un precepto de impacto general habilitador de una completa legislación dirigida a garantizar derechos digitales, entre los cuales, el de protección de datos ocuparía una posición central? Para responder este interrogante es preciso contextualizar los debates constituyentes y el desarrollo posterior de este precepto constitucional[5]. No admite discusión, a la luz de los debates constituyentes y del tenor literal del art. 18.4 CE, que este precepto, lejos de circunscribir su alcance a la consagración de un específico derecho, ha impuesto al legislador un amplio mandato para proteger y preservar el pleno ejercicio de derechos y libertades frente a lo que originalmente se denominó «la informática».

Sin embargo, no puede negarse que, tras unos titubeos iniciales provocados por la potencia omnicomprensiva del consolidado derecho a la intimidad, la principal virtualidad del art. 18.4 CE ha sido servir de anclaje constitucional al derecho de protección de datos y el Tribunal Constitucional

[5] Nadie duda que el art. 18.4 CE es deudor y bebe de las fuentes del art. 35 de la Constitución portuguesa de 1976. Existe un claro prejuicio negativo en el constituyente hacia los efectos perniciosos que pudieran derivarse del uso de la informática como lo demuestra la intervención del diputado Solé Tura: "El tema de la informática es fundamental, aunque hoy solo se encuentre en los inicios [...]. Se trata de establecer garantías de control de los controladores" (*Constitución española. Trabajos parlamentarios*, Tomo I, Madrid, Cortes Generales, 1980, pp. 1068 y ss.).

así lo ha reconocido a pesar de las resistencias iniciales (Lucas Murillo de la Cueva, 2003).

En un contexto propicio —recién aprobada la Ley Orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) que, como primera ley española de protección de datos, implementaba en nuestro país el Convenio 108 del Consejo de Europa, de 28 de enero de 1981—, e iniciándose en las instituciones comunitarias europeas los debates que llevarían a alumbrar la Directiva 95/56, el Tribunal Constitucional afirmó el carácter no subordinado a la garantía de la intimidad del *derecho fundamental a la protección de datos personales* (STC 254/93) (Villaverde Menéndez, 1994: 187-224). Esta sentencia serviría al TC para aproximarse tímidamente al contenido mínimo de este derecho fundamental: «La llamada "libertad informática" es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data)*» (Lucas, 1993)[6].

Más determinante resultó la aprobación de la Directiva 95/46 y de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) para que el TC diera el salto definitivo para consagrar finalmente un derecho fundamental autónomo a la protección de datos personales y para dotarlo de un inequívoco contenido esencial —a pesar, curiosamente, de que las SSTC 290/2000 [7] y 292/2000 [8] recayeron sobre sendos recursos de inconstitucionalidad interpuestos sobre la ya derogada LORTAD (Alguacil González, 2001: 365-385)—.

---

6 El TC reconoció las limitaciones del derecho a la intimidad —concebido con facultades negativas dirigidas a excluir intromisiones ilegítimas— para afrontar los riesgos provenientes de las nuevas tecnologías y la necesidad de empoderar al individuo para conocer la existencia, los fines y los responsables de los ficheros automatizados donde obran datos personales de un ciudadano a fin de salvaguardar los intereses protegidos por el art. 18 CE.

7 «El derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales, pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos».

8 «La peculiaridad de este derecho fundamental a la protección de datos respecto del derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

Durante casi tres décadas, el derecho a la protección de datos ha ostentado en exclusiva el honor de desarrollar el mandato del art. 18.4 CE. Durante décadas, las garantías de los derechos frente a los avances tecnológicos se han vertebrado en torno al derecho a la protección de datos al que se le ha dotado de una potencia normativa extraordinaria[9]. Sirva como ejemplo su consagración como un derecho fundamental autónomo en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea [10]. Pero este manto protector parece no dar más de sí para cubrir y amparar otras muchas amenazas y riesgos que operan, al margen de la información personal, en la realidad digital sobre derechos y libertades individuales.

En definitiva, el reconocimiento por la jurisprudencia constitucional de un derecho fundamental autónomo a la protección de datos personales ha servido de auténtica punta de lanza del mandato constitucional dirigido a los poderes públicos para limitar el uso de la tecnología en garantía de los derechos. La fuerza expansiva de este derecho ha permitido canalizar y limitar los posibles riesgos provocados por la tecnología, pero su enorme potencialidad ya no alcanza a todos los ámbitos en los que hoy se proyectan estas amenazas. Por ello, el art. 18.4 CE adquiere de nuevo sentido en toda su plenitud más allá de la acotada preocupación por garantizar la protección de datos y reclama una decidida acción legislativa dirigida a reconocer y garantizar los derechos digitales, esto es, los derechos y libertades individuales afectados por la realidad digital.

No obstante, el mandato del art. 18.4 CE adolece de las limitaciones inherentes a su propia naturaleza: una genérica habilitación al legislador para reconocer y regular derechos digitales sufrirá las debilidades propias de este rango normativo y someterá a discreción legislativa su tipología y contenidos básicos. Cuatro décadas después de producirse la visionaria decisión del constituyente, la hipotética reforma del texto constitucional sería la mejor respuesta para constitucionalizar estos derechos digitales como lo ha reivindicado el legislador orgánico en el preámbulo de la LOPDGDD. En tanto no se acometa la tarea anterior, resulta ineludible la necesidad de reconocer *nuevos derechos digitales*. El título X de la LOPDGDD responde a esta necesidad y al cumplimiento del mandato constitucional vigente. Por primera vez, un Estado

9 La abducción de este derecho fundamental, convirtiéndolo en un derecho exclusivamente europeo, ha sido abordada recientemente en Rallo Lombarte (2019b).

10 El preámbulo de la *Dichiarazione dei diritti in internet* afirma: «L'Unione europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall'articolo 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di internet, anche in una prospettiva globale».

europeo garantiza por ley derechos digitales en todos los ámbitos individuales y colectivos afectados por la tecnología. Algunas instancias internacionales y países europeos han sido pioneros en el impulso del reconocimiento de derechos digitales y, sin duda, la ley española los ha tomado como referencia.

III. DIMENSIÓN GLOBAL Y EUROPEA

El reconocimiento del derecho de protección de datos ha servido de punta de lanza en la historia del reconocimiento de los derechos digitales. El ya referido Convenio 108 del Consejo de Europa de 28 de enero de 1981 y las *Guidelines on the protection of privacy and transborder flows of personal data* adoptadas por la OCDE en 1980 supusieron el punto de partida a nivel global para afrontar los retos de la automatización. La Directiva 95/46 significó un hito en la historia de la protección de los datos al consagrar principios con plena vigencia a lo largo de dos décadas para afrontar la vertiginosa evolución tecnológica y la globalización (Zolo, 2009). Sin embargo, la Unión Europea, a la vanguardia de los avances en garantía de derechos digitales, abordó el reto de modernizar su normativa de protección de datos para, de forma principal, preservar los derechos, libertades y la dignidad humana ante los riesgos y amenazas de la realidad digital (Rallo Lombarte y García Mahamut, 2015). El propio preámbulo de la CDFUE proclamó la necesidad de «reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos» para consagrar posteriormente, en su art. 8, el derecho fundamental de protección de datos personales como instrumento relevante para alcanzar tal fin (Ruiz Miguel, 2003: 7-43; Guerrero Pico, 2005, 293-334). El Reglamento 2016/679 General de Protección de Datos (RGPD) (López Calvo, 2017, 2019), vista la debilidad que evidenciaban los tradicionales derechos instrumentales de protección de datos (acceso, rectificación, supresión y oposición) para someter al entorno tecnológico, apostó por la creación de *nuevos derechos digitales* intrínsecamente vinculados al derecho de protección de datos: a) derecho reforzado de información al usuario[11]; b) derecho al olvido (Rallo Lombarte, 2014, 2018b); c) derecho a la notificación de la rectificación o supresión de datos[12], y d) derecho a la portabilidad [13].

[11] Una manifestación contundente de este reforzamiento lo encontramos en el art. 12.1 RGPD y en el considerando 58 RGPD.

[12] Puede intuirse fácilmente el impacto de este derecho en los servicios de internet, como evidencia el art. 19 RGPD.

[13] Art. 20 RGPD y, para mejor comprender el alcance de este derecho, véase el considerando 68 RGPD.

Sin embargo, estos nuevos derechos vinculados a la protección de datos personales no satisfacen las demandas presentes en la sociedad digital. Son muchos los ámbitos personales (sistema educativo, relaciones laborales, etc.) o colectivos (ejercicio de derechos y libertades públicas, prestaciones de servicios, etc.) en los que la necesidad de garantizar derechos digitales se hace patente. Y así lo corroboran algunos desarrollos legislativos nacionales.

Otras instancias europeas no permanecieron impasibles ante estos desarrollos normativos dirigidos a garantizar derechos digitales. El Parlamento Europeo ya había adoptado el 26 de marzo de 2009 su Recomendación 2008/2160(INI) sobre el refuerzo de la seguridad y de las libertades fundamentales en internet[14] requiriendo del Consejo acciones dirigidas a posibilitar un acceso pleno y seguro a internet para todos, un compromiso firme de lucha contra la ciberdelincuencia y una protección absoluta y promoción de las libertades fundamentales en internet[15]. Mayor impacto adquirirá la Recomendación CM/REC (2014)6, adoptada por el Consejo de Ministros del Consejo de Europa el 16 de abril de 2014, sobre una *Guía de los derechos humanos para los usuarios de internet* [16], que recordaba la obligación de los Estados miembros de garantizar los derechos y las libertades fundamentales consagrados en el Convenio Europeo de Derechos Humanos también en el contexto de internet. A este efecto, recordaba el Consejo de Europa que «internet tiene características de servicio público» dada la progresiva dependencia de todos los agentes públicos y privados en sus actividades y habida cuenta de que todos ellos «tienen una expectativa legítima de que sus servicios sean accesibles, ofrecidos sin discriminación, asequibles, seguros, fiables y continuos»; de forma que debería quedar proscrita toda injerencia ilícita, innecesaria o desproporcionada en el ejercicio de los derechos humanos y las libertades fundamentales al usar internet. Al tiempo que se adoptan las anteriores iniciativas europeas, se producen otros impulsos para el reconocimiento de derechos digitales con carácter global[17], como la Resolución del Consejo de Derechos

[14] Disponible en: http://bit.ly/397BXqW.

[15] Resultan especialmente valiosas las siguientes consideraciones incluidas en la Recomendación: «La «identidad digital» se está convirtiendo en parte integrante de nuestro «yo» y, por lo tanto, merece protección adecuada y eficaz contra las intrusiones de agentes privados o públicos, por lo que el conjunto particular de datos que está orgánicamente vinculado a la «identidad digital» de un individuo debe definirse y protegerse, y todos sus elementos deben ser considerados derechos personales, no económicos, no negociables e inalienables», disponible en: http://bit.ly/397BXqW.

[16] Disponible en: https://rm.coe.int/16804c177e.

[17] Tiene gran interés la *Carta de derechos humanos y principios para internet* de 2015 elaborada por *internet Rights & Principles Coalition* del Foro para la Gobernanza

Humanos de Naciones Unidas de 27 de junio de 2016 sobre Promoción, Protección y Disfrute de los Derechos Humanos en internet[18].

IV. ESTRATEGIAS NACIONALES: LA EXPERIENCIA FRANCESA COMO REFERENCIA

Estos tímidos impulsos globales se han visto acompañados de otras estrategias nacionales que han tenido alcance diverso. En 2014, la Conferencia Net Mundial celebrada en Brasil fue el entorno elegido para anunciar la que pretenciosamente se dio en llamar *la primera Constitución de internet del mundo* —cuando, en realidad, se trataba de la Ley brasileña 12 965, de 23 de abril de 2014, que establecía los principios, garantías, derechos y deberes para el uso de internet en Brasil, también denominada *marco civil de internet* [19], con muy escasas novedades sobre las regulaciones ya vigentes en otros muchos países, particularmente europeos—. En Italia (Nannipieri, 2015) encontramos una primera iniciativa nacional de interés e impacto social incuestionable pero, al tiempo, de nulo alcance jurídico: la *Dichiarazione dei diritti in internet* de 28 de julio de 2015, elaborada y aprobada por la Commissione per i diritti e i doveri relativi ad internet de la Cámara de Diputados [20].

Sin embargo, el salto cualitativo lo encontramos en Francia, donde se supera la fase del reconocimiento declarativo de principios y derechos digitales para consagrar auténticas obligaciones y derechos. La Loi n.° 2016-1321 du 7 octobre 2016 pour une République numérique[21] constituye una referencia inexcusable pues aborda un amplio y sistemático catálogo de derechos digitales: a) derecho de acceso a datos públicos y de interés general; b) derecho de

de internet de las Naciones Unidas (http://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_internet.pdf).

18 Disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf.

19 *Marco civil brasileño de internet* ; Cámara de Diputados, Documentación, Brasilia, 2015 (https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20_internet.pdf).

20 La Declaración termina con unas sugerentes consideraciones sobre el *gobierno de la red*: «internet richiede regole conformi alla sua dimensione universale e sovranazionale per […] evitare che la sua disciplina dipenda dal potere esercitato da soggetti dotati di maggiore forza economica […]. La costituzione di autorità nazionali e sovranazionali è indispensabile per garantire effettivamente il rispetto dei criteri indicati, anche attraverso una valutazione di conformità delle nuove norme ai principi di questa Dichiarazione».

21 Disponible en: http://bit.ly/2vcmash.

acceso seguro para investigadores y estadísticos públicos; c) derecho de acceso libre a los resultados de la investigación pública; d) derecho a la neutralidad de la red; e) derecho a la portabilidad; f) derecho a información leal; g) derecho a la protección de datos personales; h) penalización de la revancha pornográfica que se produce cuando se publica contra alguien imágenes eróticas o pornográficas; i) derecho a la muerte digital decidiendo el destino de la información personal *online* ante servicios de internet y terceros de confianza; j) derecho al mantenimiento de la conexión a internet de las personas económicamente más desfavorecidas en caso de mora o impago, y k) garantía de accesibilidad digital de las Administraciones públicas.

Francia se ha convertido en un modelo de referencia y su legislación opera en todos los ámbitos: garantizando la dimensión prestacional mediante la neutralidad de la red, con un derecho de acceso universal sin brechas socioeconómicas, geográficas o por condiciones de vulnerabilidad; promoviendo el acceso al conocimiento digital mediante una estrategia decidida de *open data*; fortaleciendo derechos tradicionales como el de protección de datos o el secreto de las comunicaciones; incidiendo en el ámbito laboral mediante el derecho a la desconexión; persiguiendo conductas delictivas, y garantizando nuevos derechos como el de portabilidad o la muerte digital. La relevancia de estas iniciativas radica en que los poderes públicos franceses, lejos de sucumbir a los ineficientes impulsos autoregulatorios, han otorgado rango legal a estos derechos y a las obligaciones que derivan de los mismos. El título X de la LOPDGDD constituye «un buen punto de partida para abordar la actualización de nuestros derechos en la era digital» (Barrio Andrés, 2018, 2019) pues aborda idéntico reto al consagrar un detallado sistema de garantía de derechos digitales que pasamos a analizar.

V. DIGNIDAD, IGUALDAD DE OPORTUNIDADES E INTERNET COMO SERVICIO PÚBLICO

El acceso a internet constituye hoy una condición indispensable para desarrollar libremente la personalidad y salvaguardar la dignidad de los individuos[22]. Acceder a internet supone garantizar la igualdad de oportunidades de las personas en sus distintas etapas de la vida. internet ya no es una herramienta cuyo uso pueda reservarse exclusivamente para ejercer actividades sectoriales o exclusivas. Un acceso universal a internet solo puede garantizarse desde su consideración como servicio público que debe ser preservado por los

[22] Un primer análisis de esta cuestión fue abordado en Rallo Lombarte (2019a: 29-33).

poderes públicos. Por ello, el art. 81 LOPDGDD proclama el derecho de todas las personas a acceder a internet independientemente de su condición personal, social, económica o geográfica.

Existe una conciencia social indudable de que para preservar derechos o condiciones de vida básicas propias de una sociedad desarrollada (Frosini, 2011: 1-17) es indispensable superar la exclusividad del uso de internet y garantizar su consideración como un auténtico servicio público (Barrio, 2017b) sin el cual el riesgo de exclusión social está servido. El carácter *universal* de internet implica su disfrute por parte de cualquier individuo, independientemente de las circunstancias económicas que lo envuelvan de carácter económico, social, geográfico, etc. Pero no basta un reconocimiento genérico que preserve su uso sin que este responda a unos estándares básicos de *calidad* que impidan el riesgo de discriminaciones de carácter técnico o social (Pisa, 2010). Son numerosos los supuestos en los que cabe identificar una potencial discriminación en el uso de internet. Basta con contraponer realidades como el acceso de hombres y el de mujeres (Castaño, 2008), el de entornos urbanos frente a rurales, el de personas mayores frente a los rangos de edad medios o el de la población general frente al de las personas con discapacidad o necesidades especiales. La superación de estas brechas digitales no puede dejarse en manos de los operadores, sino que requiere de *políticas de impulso* por parte de los poderes públicos que atiendan a las disfunciones que el mercado inexorablemente puede provocar al buscar la maximización del beneficio económico en detrimento de las necesidades humanas inherentes a la igualdad de oportunidades. Por ello, un acceso universal a internet sin discriminaciones técnicas o socioeconómicas impone límites a las actividades comerciales de los operadores y servicios de internet (García Mexía, 2017). El denominado «derecho a la neutralidad de internet» (Berners-Lee, 2010; Pérez Martínez, 2011; Barata, 2012; González San Juan, 2016)[23], también proclamado en el art. 80 LOPDGDD, busca preservar la esencia igualitaria con la que nació internet frente a la pretensión de los operadores y prestadores de servicios de diferenciar el trato a los usuarios en función de sus necesidades y, por ende, de sus

[23] La evolución de internet y del modelo de negocio de los operadores de telecomunicaciones y de los prestadores de servicios de internet ha abierto un debate actual sobre la posibilidad de diferenciar ofertas en función de las necesidades y capacidades, fundamentalmente económicas, de los destinatarios de dichos servicios. Se debate sobre la posibilidad de ofrecer internet a *varias velocidades,* lo que en la práctica significaría que la calidad de uso de dicho servicio variara en función de las capacidades económicas de los usuarios, provocando así una estratificación social en el disfrute de un servicio y, por ende, una negación de la igualdad de oportunidades en los beneficios que comporta su uso.

posibilidades económicas. Las ofertas diferenciadas de servicios en internet, vinculando calidad técnica con recursos económicos, supondrían una herida mortal en el corazón de un servicio que ha contribuido indiscutiblemente a una democratización del flujo de la información y del conocimiento. La transparencia en la oferta de servicios constituye, sin duda, un elemento inescindible para proscribir discriminaciones de carácter técnico o económico.

La seguridad en el uso de la red es un elemento consustancial a su uso, expansión y pervivencia. La seguridad de las comunicaciones en internet constituye una condición básica para generar confianza y credibilidad a riesgo de debilitar sus potencialidades y quebrar su cometido existencial. El art. 82 LOPDGDD proscribe, en última instancia, accesos indeseados que pongan en riesgo la calidad de los servicios que se ofrecen en la red y, al mismo tiempo, preserva la privacidad en la transmisión de contenidos que afectan a la esfera individual[24].

La dimensión prestacional del derecho de acceso a internet no se agota, sin embargo, con la satisfacción del deber de los poderes públicos de adoptar las medidas necesarias para facilitar directa (bono social, etc.) o indirectamente (imponiendo obligaciones a los operadores, etc.) los recursos técnicos o económicos necesarios para la utilización de internet. Si las primeras décadas de uso de internet se han caracterizado por el autodidactismo sustentado en la intuición del usuario y por el avance de una tecnología que de los proveedores de servicios procuran que sea de uso *amable* (*friendly*), lo cierto es que todo ello no garantiza suficientemente un acceso suficientemente consciente y riguroso a las herramientas digitales. Los poderes públicos no pueden ser ajenos a la necesidad de procurar los medios necesarios para formar a los usuarios en el uso, potencialidad y riesgos de unas herramientas digitales cuya complejidad y sofisticación resulta inherente al entorno digital. Las sucesivas generaciones digitales requieren de una capacitación que les permita obtener el máximo aprovechamiento y beneficio de los instrumentos digitales y el sistema educativo no puede permanecer ajeno a esta necesidad, sino, más bien al contrario, debe insertar en sus contenidos mínimos el carácter transversal del impacto digital. Por ello, el art. 83 LOPDGDD va más allá de una genérica mención al derecho a la educación digital para imponer específicas obligaciones que posibiliten un escenario futuro en el que los ciudadanos realicen un

[24] La seguridad de internet implica, sin duda, a los poderes públicos que deben actuar para preservar este derecho frente a las amenazas crecientes que operan más allá de acciones indebidas de carácter limitado, pero concierne particularmente a los proveedores de servicios, a los que les resultará exigible la máxima diligencia en preservar este mandato y facilitar a los usuarios la información necesaria para el ejercicio de sus derechos.

uso de la tecnología seguro, consciente y garantista[25]. No se trata únicamente de que el sistema educativo procure, en todos sus niveles, el aprendizaje en la utilización de los medios digitales, sino que dicho uso debe estar presidido e inspirado por unos objetivos y principios que lo orienten: en respeto de la dignidad humana, de los valores constitucionales, de los derechos fundamentales y, particularmente, la garantía de la intimidad personal y familiar y la protección de datos personales. No resulta suficiente un supuesto aprendizaje neutro de los medios y servicios existentes en internet. La experiencia de las últimas décadas de generalización de medios digitales muestra la perentoria necesidad de que su manejo tenga muy presente un uso consciente y respetuoso con los derechos y libertades propios y con los valores constitucionales que demasiadas veces pueden ponerse en riesgo cuando se trivializa o banaliza el uso compulsivo de los servicios digitales.

Los usuarios van creando su propia historia digital que no puede quedar vinculada a servicios específicos. Así lo advertía el 22 de junio de 2010 Viviane Reding, vicepresidenta de la Comisión Europea y comisaria de Justicia, Derechos Fundamentales y Ciudadanía, cuando afirmaba: «Si tengo mis preciosas fotos almacenadas en cualquier sitio de la nube, ¿qué sucede si quiero cambiar a otro proveedor?»[26]. La Comisión Europea se propuso estudiar los medios y reformas normativas necesarios para lograr el pretendido reforzamiento del control sobre los datos personales en el mundo *online* garantizando la portabilidad de los datos mediante un derecho explícito a retirar datos como fotografías o listas de amigos de una aplicación o de un servicio, de modo que los datos retirados pudieran transferirse a otra aplicación o servicio, siempre que ello fuera técnicamente posible y sin que los responsables del tratamiento lo obstaculizaran. Los arts. 20 RGPD y 17 LOPDGDD culminaron esta voluntad al proclamar el «derecho a la portabilidad de los datos», esto es, el derecho a recibir los datos personales que se hayan facilitado en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos sin impedimentos cuando medie consentimiento, contrato y un tratamiento automatizado. Sin embargo, estos preceptos solo posibilitan la transmisión de datos personales en cualquier formato automatizado (también redes sociales y servicios equivalentes), pero no agotan la necesidad de amparar el derecho de todo usuario de dichos servicios a obtener la totalidad de los contenidos que hayan incorporado a dichos

[25] Algunas de las numerosas iniciativas dirigidas a este fin: *Resolución sobre la educación digital para todos*, 35th International Conference of Data Protection and Privacy Commissioners, Wasaw, 23-26 septiembre, 2013; Plan de Acción de Educación Digital, de 17 de enero de 2018 [COM (2018)].

[26] «Building Trust in Europe's Online Single Market», speech at the American Chamber of Commerce to the EU, Brussels, 22 June 2010 (http://bit.ly/2urbi9O).

servicios y no solo de aquellos en los que existan datos personales. Por esta razón, el art. 95 LOPDGDD (derecho de portabilidad en servicios de redes sociales y servicios equivalentes) extiende a todos los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes el derecho a recibir y transmitir cualesquiera contenidos que hubieran facilitado a los prestadores de dichos servicios, de forma que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

VI. LIBERTAD DE EXPRESIÓN Y MEDIOS DE COMUNICACIÓN: LÍMITES

Internet constituye la columna vertebral de la sociedad del conocimiento y de la información. Pocos avances científico-tecnológicos en la historia de la humanidad han resultado tan revolucionarios y determinantes para la conducta individual y colectiva y tan decisorios para multiplicar exponencialmente las capacidades humanas de adquisición de conocimiento a través de la información. Nunca en la historia de la humanidad resultó imaginable que pudiera existir un espacio para la transmisión de ideas, opiniones e informaciones de tal magnitud (Cotino Hueso, 2007). Su dimensión global, planetaria, universal y permanente otorga a la libertad de expresión y al derecho a la información una dimensión e impacto hasta la fecha desconocidos (Rallo Lombarte y Martínez, 2013a: 407-423). No resulta extraño o incomprensible que los beneficios aportados por la red al fortalecimiento de las libertades informativas en las democracias contemporáneas hayan venido acompañados de grandes evangelistas que loan las virtudes de la red y defienden a ultranza sus elementos definitorios originales: un espacio de libertad y apertura sin límites. Sin embargo, la tentación de reducir la consideración de internet a su mera intelección como un medio de comunicación de información devalúa su alcance potencial y, al tiempo, desdibuja los perfiles propios del ejercicio de las libertades informativas (libertad de expresión y derecho a la información) a través de internet. La evolución del uso de internet ha llevado a advertir sobre los riesgos que acompañan convertir la Red en un espacio de impunidad en el que el ejercicio de la libertad de expresión o el derecho de información no se vean sometidos a las reglas generales que rigen su ejercicio en las sociedades democráticas (Cotino Hueso, 2011; Corredoira Alfonso y Cotino Hueso, 2013).

Apenas tres décadas de existencia de internet han bastado para advertir sobre la necesidad de introducir normas que coadyuven a preservar la calidad de contenidos y a salvaguardar los derechos y libertades en riesgo frente a contenidos que vulneren la esfera propia de la dignidad humana (Fernández

Esteban, 1999: 149-169). A falta de instrumentos supranacionales, los poderes públicos estatales, de forma progresiva, están introduciendo mecanismos de reacción y reparación de las conductas que en internet merecen ser calificadas como ilícitas por atentar contra el sistema de derechos y libertades acrisolado durante los dos últimos siglos y, en particular, contra aquellos, como el derecho a la privacidad, especialmente vulnerables.

La libertad de expresión tiene hoy en internet su canal predilecto y merece protección y salvaguarda. La difusión de información en internet constituye un elemento axial sobre el que se asientan las democracias contemporáneas[27]. En consecuencia, sin paliativos ni matices, el art. 85 LOPDGDD proclama el derecho de «todos a la libertad de expresión en internet» y, también, a recibir y difundir información veraz con los únicos límites que, con la preceptiva intervención judicial, impone la legislación penal (López Ortega, 2001: 83-126). Además de los medios de comunicación, cualquier individuo tiene derecho a difundir y recibir información veraz. El llamado «periodismo ciudadano» (García-Alonso, 2006: 251-262) evidencia que en la red cualquier usuario está en condiciones de ejercer los derechos informativos constitucionalmente reconocidos. Ahora bien, los medios de comunicación tradicionales o sus versiones digitales siguen jugando un rol singular en la transmisión de información, por lo que el ordenamiento debe procurarles una atención especial más allá del reconocimiento de la universalización de capacidades informativas en la red (Bárcena, 2016: 141-168) que han multiplicado la demanda de reacción frente a contenidos que transgreden la exigencia de veracidad constitucionalmente amparada. Por esta razón, el art. 85.1 LOPDGDD busca posibilitar la depuración reactiva (y no preventiva) de datos (personales o no) publicados que contravienen el deber de exactitud y frente a los cuales el ordenamiento ya contempla su revisión a través del ejercicio del derecho de rectificación. En consecuencia, esta norma pretende posibilitar el ejercicio efectivo del derecho de rectificación en internet y, además, extender a usuarios de redes sociales y servicios equivalentes los requisitos y procedimientos previstos en la LO 2/1984 (hasta la fecha únicamente predicables de los editores de medios de comunicación) en tanto autores-editores de dichos contenidos inexactos.

Nadie duda de que el derecho de rectificación garantizado por la LO 2/1984 resulta plenamente aplicable a los medios de comunicación digitales. Sin embargo, esta afirmación ha chocado con dos dificultades de las que debemos ser conscientes. Por un lado, la identificación de los denominados *medios de comunicación digitales* no siempre resulta pacífica. Por otro, a falta de norma expresa que lo explicitase, la consideración de los usuarios de redes sociales o

[27] Esta cuestión ya fue analizada en Rallo Lombarte (2019a: 37-43).

servicios equivalentes como editores de contenidos sujetos al ejercicio del derecho de rectificación (Benito García, 2004)[28] tampoco gozaba de suficiente consenso. Por ello, la principal novedad del art. 85.1 radica en extender los requisitos y procedimientos de la LO 2/1984 a cualquier usuario de redes que publique o difunda hechos inexactos que puedan causar perjuicio a quien decide ejercer el derecho de rectificación. Este precepto no otorga a los proveedores de servicios de internet facultad alguna de censura *ex ante* o *ex post*, preventiva o reactiva. Esta norma excluye cualquier actuación valorativa por parte de los responsables de redes sociales o servicios equivalentes y únicamente los conmina a proveer los medios necesarios para que los potenciales damnificados por una información o contenido inexacto puedan ejercer el derecho de rectificación ante sus autores. Esto es, se impone una obligación meramente instrumental a los responsables de redes sociales o servicios equivalentes consistente en la adopción de protocolos adecuados que posibiliten el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la LO 2/1984.

Siendo cierto que el derecho de rectificación resulta plenamente predicable de los medios de comunicación digitales, lo cierto es que su concreción no siempre resulta pacífica. Por ello, el art. 85 aporta un mecanismo que debiera satisfacer, sin conflicto, dicho derecho: «Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original». La técnica de los avisos aclaratorios en los medios de comunicación *online* se ha ido progresivamente consolidando en la jurisprudencia europea dada su fácil viabilidad técnica para aportar mayor calidad al producto informativo y satisfacer las exigencias de actualización de contenidos[29]. Así, el art. 86 («Derecho a la actualización de informaciones en medios de comunicación digitales»)

[28] De particular interés, el análisis y propuestas sobre la necesidad de adaptar la Ley Orgánica Reguladora del Derecho de Rectificación a la realidad *online* (pp. 180-234).

[29] En el caso *Times Newspapers vs. UK*, el TEDH sentenció el 10 de marzo de 2009 que la prensa tenía el deber de garantizar la exactitud de la información histórica publicada en internet, lo que avalaba incluir un *aviso de actualización*: «En estas circunstancias, el TEDH, al igual que el Tribunal de Apelación, considera que la obligación de *publicar un aviso* junto a un artículo archivado en internet, advirtiendo de que su publicación en la prensa escrita ha sido objeto de una acción de difamación, *no constituye una desproporcionada interferencia en el derecho a la libertad de expresión*».

proclama que toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio. En particular, se garantiza la inclusión de dicho aviso cuando las informaciones originales refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. Estamos ante una técnica que ya resulta práctica común en numerosos medios de comunicación digitales y que se contempla en algunos de sus libros de estilo[30].

El establecimiento de límites al derecho a informar en internet ha conocido, en la última década, un elemento conflictual al emerger un nuevo derecho de dimensiones imprecisas: el derecho al olvido. Este derecho no tiene una proyección exclusiva en los medios de comunicación digitales. Más bien al contrario. Su verdadero alcance se proyecta sobre datos personales publicados en cualesquiera plataformas digitales. La depuración en internet de informaciones personales cuya finalidad original caduca con el transcurso del tiempo adquiere pleno sentido en cualquier ámbito de internet. Sin embargo, cuando dichas informaciones personales gozan de interés público, el conflicto entre el supuesto derecho del titular de las mismas a su supresión y el derecho de la sociedad a acceder a las mismas queda servido y exige de instrumentos para resolverlo.

El derecho al olvido (Rallo Lombarte, 2014, 2018b) ha sido consagrado jurídicamente por primera vez en el art. 17 RGPD: una referencia explícita, pero equívoca y cuestionable. La redacción final del art. 17 RGPD no ha despejado las críticas que se formularon al proyecto inicial al no establecerse una neta diferenciación entre el derecho de supresión y el derecho al olvido y, más bien al contrario, al calificarlos como categorías idénticas. El derecho al olvido ha quedado claramente subsumido en el derecho de supresión a pesar de que el proyecto original parecía aventurar dos derechos diferentes en su rúbrica —«derecho al olvido y de supresión»—. El texto definitivo adopta un título que inequívocamente incluye, sin diferenciarlos, el derecho al olvido en el derecho de supresión —«derecho de supresión ("derecho al olvido")»—. En definitiva, el RGPD utiliza de forma indistinta y como sinónimos ambos términos.

Ahora bien, el art. 17.2 RGPD impone la obligación de informar a quienes acceden a datos personales cuya supresión ha sido solicitada para limitar el

[30] Por ejemplo, el *Libro de estilo de El País* (Aguilar, Madrid, 2014, pp. 37-38).

impacto de esta difusión masiva de datos personales. Se trata, sin duda, de la única referencia del precepto de carácter innovador que se imbrica con la naturaleza sustancial del derecho al olvido dirigida a minimizar el impacto del alcance perenne y universal de las informaciones que se difunden en internet. Pero, como advierte el precepto, las limitaciones técnicas existentes imponen una visión realista y práctica limitativa del derecho al olvido atendiendo a la tecnología disponible y al coste de implementación[31]. Así las cosas, la interpretación conjunta del art. 17 RGPD y de los considerandos 65 y 66 permite concluir que el art. 17 RGPD únicamente consagra el tradicional derecho de supresión, mientras que la novedosa referencia al derecho al olvido únicamente se materializa en una manifestación básica: informar a terceros sobre la petición de supresión y cancelar réplicas *online*. Si bien la literalidad del RGPD apenas innova el alcance normativo del derecho al olvido, lo cierto es que este novedoso derecho ha forjado su existencia sobre las vigas maestras sobre las que se asienta el derecho de supresión que resulta explicitado y notablemente reforzado en el RGPD. De forma que el art. 17 RGPD ni excluye la doctrina establecida por la Sentencia del TJUE de 13 de mayo de 2014 (C-131/12, caso *Google v. Spain*), que conforma el ni siquiera nombrado derecho al olvido, ni impide, en aras a la certeza y seguridad jurídica, la consolidación legal en un Estado miembro de dicha doctrina jurisprudencial (Rallo, 2017b). Es más, la STC 58/2018, de 4 de junio, haciéndose eco de la anterior sentencia del TJUE, no ha dudado en proclamar el «reconocimiento expreso del derecho al olvido como facultad inherente al derecho a la protección de datos personales y, por tanto, como derecho fundamental». Y, por ello, precisamente, los arts. 93 y 94 LOPDGDD recopilan legislativamente la doctrina establecida por el TJUE y el TC tanto en el supuesto concreto objeto de solución judicial («Derecho al olvido en búsquedas de internet») como en su incuestionable aplicación a otros ámbitos («Derecho al olvido en servicios de redes sociales y servicios equivalentes»).

El art. 93 no altera los contornos jurisprudenciales del derecho al olvido. Todo lo contrario: se limita a consagrar escrupulosamente los rasgos informadores del derecho al olvido ante las búsquedas de internet impuestos por la Sentencia del TJUE de 13 de mayo de 2014 (C-131/12, Caso *Google v. Spain*). Dicha sentencia, como ahora establece el art. 93, ampara: a) la supresión de

[31] Los límites del derecho de supresión (derecho al olvido) aparecen claramente explicitados en el art. 17.3 RGPD: a) el derecho a la libertad de expresión e información; b) el cumplimiento de una obligación legal o el cumplimiento de una misión de interés público; c) la salud pública; d) archivo público, investigación científica o histórica o fines estadísticos, y e) la defensa de reclamaciones.

resultados de búsquedas cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en internet; b) el reconocimiento de este derecho sin necesidad de la previa supresión de las informaciones publicadas en el sitio web, puesto que este derecho subsiste aunque sea lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo, y c) el ejercicio del derecho al olvido sin necesidad de supresión de los datos existentes en el sitio web que los acogió originalmente, de tal forma que no se impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Ahora bien, la doctrina anterior recayó sobre el supuesto de la supresión de resultados de buscadores de internet y, por ello, resulta relevante preguntarse si esta jurisprudencia resulta trasladable a cualquier ámbito de internet y, particularmente, a las redes sociales (Gil Antón, 2012: 209-255) y servicios equivalentes. La respuesta solo puede ser afirmativa. Por ello, el art. 94 («Derecho al olvido en servicios de redes sociales y servicios equivalentes») establece que «toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes». El derecho al olvido en redes sociales y servicios equivalentes de internet supone una concreción del derecho de supresión amparada por el principio de calidad de los datos que resulta especialmente afectado por el transcurso del tiempo (exactitud, pertinencia, actualización) y que se instrumentaliza tanto por el derecho de supresión como de rectificación y por el derecho de oposición que atiende a las circunstancias personales que afectan al solicitante. Los límites al ejercicio de este derecho se encuentran bien en el interés público de los datos personales, bien en la naturaleza personal o doméstica de la actividad que viene excluida de su ámbito de aplicación por el RGPD. La manifestación incondicionada del derecho al olvido en redes sociales se plasma en el ejercicio del mismo, no sometido a condición alguna, por parte de quien facilitó los datos en su minoría de edad.

VII. RELACIONES LABORALES Y DIGITALIZACIÓN

El mundo del trabajo ha sufrido en las últimas décadas una transformación extraordinaria, provocada por la digitalización de todas las actividades que lo envuelven y, singularmente, por su impacto en las relaciones laborales entre

empleador y empleado[32]. Las relaciones laborales se han visto singularmente condicionadas por la introducción de dispositivos digitales en el ámbito laboral dirigidos a controlar la actividad laboral o a procurar instrumentos digitales a los trabajadores que maximizan su productividad. De hecho, la utilización de ordenadores o teléfonos móviles, de carácter corporativo o personal, ha tenido un impacto singular en el disfrute de derechos individuales por los trabajadores y, especialmente, de su derecho a la intimidad personal y familiar. Lo problemático del uso de estas herramientas no solo se ha proyectado sobre el disfrute de derechos, sino que ha adquirido, incluso, tintes dramáticos al poner en riesgo la salud al imponerse la disponibilidad plena y permanente de los trabajadores en su hacer laboral.

No puede extrañar, en consecuencia, el éxito adquirido por un novedoso «derecho a la desconexión digital» que responde a una demanda global y que algunos países han ido incorporando progresivamente a sus ordenamientos. También lo hace España al reconocerlo en el art. 88 LOPDGDD por constituir un ejemplo paradigmático del grado de intrusión protagonizado por la tecnología en la vida cotidiana de las personas (Alemán Páez, 2017: 12-33; Cialti, 2017: 163-181). Como se ha advertido, las patologías que acompañan a esta intrusión ya no solo afectan al disfrute de derechos, sino que generan, incluso, riesgos para la salud (Naval Durán *et al.*, 2016: 73-90). Esta causa ha llevado a países vecinos (Francia[33], originalmente, pero ya extendida a Italia[34] o Bélgica[35]) a regular el derecho de los trabajadores a ver garantizado su tiempo de descanso y vida privada sin la intrusión protagonizada por la omnipresencia de lo digital en el mundo laboral.

En nuestro país[36], parte de la doctrina ha considerado que el derecho a la desconexión digital ya tenía amparo en el derecho al descanso legalmente

---

32 Unas consideraciones previas ya fueron tratadas en Rallo Lombarte (2019: 43-47).

33 La norma española está inequívocamente influida por la Loi n.° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels que, con efectos desde el 1 de enero de 2017, introdujo por primera vez el derecho a la desconexión digital al modificar el art. 55.I.2.º de la Loi 2016-1088 e introducir un nuevo apartado 7 en el art. L. 2242-8 del Código de Trabajo francés.

34 Así lo contempla el apartado 1 del art. 19 («Forma e recesso») de la L. 22 maggio 2017, n. 81 (1). Un análisis de este precepto en Di Meo (2017).

35 Así lo establece el art. 16 («Concertation sur la déconnexion et l'utilisation des moyens de communication digitaux») de la Loi du 26 mars 2018 relative au renforcement de la croissance économique et de la cohésion social.

36 Con anterioridad a la adopción de esta norma, algunas grandes empresas ya habían establecido políticas internas dirigidas a garantizar este derecho. El 22 de junio de

establecido (Molina Navarrete, 2017: 249-283; Vallecillo Gámez, 2017: 167-178) pero lo cierto es que, a falta de su explicitación normativa, la realidad muestra la nula preservación de este derecho y su dificultosa exigibilidad. Por ello, este art. 88.1 reconoce a trabajadores y empleados públicos el derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

A nadie escapa, sin embargo, que este derecho no puede generalizarse sin adecuarlo a un mundo laboral inclusivo de realidades muy diferentes que demandan de un alto grado de flexibilidad y acuerdo entre los agentes sociales. Por ello, el art. 88.2 establece un marco flexible y negocial que permita su adecuación a las circunstancias concretas: «Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores» (Quílez Moreno, 2018: 305-324). Pero la remisión a la negociación colectiva[37] entre empresa y trabajadores no debe impedir la visualización de una auténtica obligación impuesta a los empleadores, y judicialmente fiscalizable, para garantizar este derecho de forma efectiva (Taléns Visconti, 2018: 193-208). Así, el art. 88.3 añade: «El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática» (Aragüez Valenzuela, 2017: 169-190; Naranjo Colorado, 2017: 49-57). Este precepto insiste en preservar el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

No pocas voces han alertado sobre la posible debilidad (incluso, nulidad) de los efectos jurídicos del incumplimiento por el empleador del derecho a la desconexión digital. Pero estas denuncias carecen de fundamento en tanto el legislador ha impuesto una obligación al empleador y ha reconocido un

2018, el Banco Santander y los sindicatos alcanzaron un principio de acuerdo para garantizar la desconexión digital de sus trabajadores. El 23 de noviembre de 2018 la dirección de Telefónica anunció la firma con UGT y CC. OO. de un documento de intenciones reconociendo el derecho a la desconexión digital.

37 Art. 14 del convenio colectivo del Grupo Axa. El convenio colectivo de la ONCE también lo contempla.

derecho a los trabajadores cuya efectividad resultará plenamente exigible, por ejemplo, ante la jurisdicción social. No resulta difícil imaginar el supuesto del despido de un trabajador sustentado en el incumplimiento de obligaciones laborales por no atender instrucciones o requerimientos del empleador transmitido a través de dispositivos digitales fuera de la jornada laboral o en tiempo vacacional. La fácil prueba de estas circunstancias convertiría en improcedente dicho despido y provocaría los efectos jurídicos derivadas de tal consideración.

Más allá del uso de estos dispositivos y su impacto en la productividad laboral, otra problemática de amplio impacto en los derechos del trabajador (particularmente, el derecho a la intimidad) es la derivada de las posibilidades de control, fiscalización e intervención de los dispositivos digitales (ordenador, teléfono móvil, etc.) puestos a disposición del trabajador por el empleador para el desarrollo de su actividad laboral. Esta realidad aboca a un inevitable conflicto entre el legítimo derecho del empleador para verificar el cumplimiento de las obligaciones laborales del trabajador (también, para supervisar la integridad técnica de los dispositivos digitales) y el derecho a la privacidad de los trabajadores, máxime cuando el empleado los viene utilizando, con consentimiento o no del empleador, para actividades que atañen exclusivamente a su vida privada. La ponderación de este conflicto ya ha obtenido una respuesta en la jurisprudencia ordinaria y constitucional asentada sobre tres reglas esenciales: a) la legitimidad del empleador para realizar el control mencionado; b) la exigencia de una información previa al trabajador sobre el alcance de la supervisión del empleador y las condiciones de uso privado de las herramientas digitales, y c) la existencia de unas condiciones básicas de privacidad del trabajador que el empleador debe respetar (Rodríguez Escanciano, 2015; Marín Alonso, 2004: 95-122; Manrique López, 2011: 169-182; Carrizosa Prieto, 2012: 251-267; Sáez Lara, 2017: 185-221; Cabeza Pereiro, 2018: 13-36; Rodríguez Cardo, 2014: 167-197)[38]. En otras palabras, el empleador

[38] Preservando la doctrina constitucional reseñada, el art. 87 ha consagrado el derecho a la intimidad de los trabajadores en el uso de dispositivos digitales facilitados por el empleador en los siguientes términos: a) los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador; b) el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos; c) los empleadores deberán establecer —en su caso, con la participación de los representantes de los trabajadores— criterios de utilización de los dispositivos digitales respetando los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos

tiene derecho a acceder a los contenidos de los dispositivos digitales que pone a disposición de sus trabajadores siempre que les informe con anterioridad de tal posibilidad, pero con un límite: el respeto a unos estándares básicos de privacidad inherentes a los usos privados socialmente aceptados en la utilización de estos dispositivos.

Ahora bien, los riesgos para los empleados derivados del uso de dispositivos digitales por el empleador tienen otras manifestaciones especialmente problemáticas cuando la intimidad de los trabajadores se ve amenazada por la utilización de dispositivos de videovigilancia, de grabación de sonidos o de geolocalización. La actuación de control del empleador para garantizar las obligaciones laborales requiere de reglas y limitaciones que modulen esta facultad de control empresarial para adecuarla a los usos y convenciones que amparan unas expectativas básicas de intimidad de los trabajadores.

Los arts. 89 y 90 reconocen la facultad de los empleadores para tratar imágenes o datos obtenidos a través de sistemas de cámaras, videocámaras y de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública (Goñi Sein, 2007, 2009: 11-58; Gude Fernández, 2014: 109-134; Jiménez-Castellanos Ballesteros, 2017: 129-156). Pero, al mismo tiempo, imponen a los empleadores la obligación de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes. Una información previa y solvente a los trabajadores se convierte en una exigencia previa para legitimar la intervención empresarial, esto es, una auténtica clave de bóveda del sistema de garantías de los trabajadores frente al control empresarial.

Hay que reconocer, sin embargo, que los conflictos derivados de la utilización de cámaras de vigilancia en el ámbito laboral están lejos de desaparecer y los criterios jurisprudenciales en torno a su legitimidad no resultan aun pacíficos como lo han evidenciado recientes pronunciamientos del TEDH recaídos en el caso *López Ribalda*. Una cadena de supermercados, tras verificar desfases entre las existencias y las ventas, instaló cámaras de videovigilancia

reconocidos constitucional y legalmente; d) el acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados, y e) los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

con las que se demostró el comportamiento irregular de cinco trabajadoras que fueron despedidas. En enero de 2019 el TEDH dictó una primera sentencia que estimó ilícita esta medida ante la falta de proporcionalidad por ausencia de información previa, explícita, clara y precisa sobre instalación de las cámaras a los trabajadores, pero esta sentencia fue revisada y revocada por la Gran Sala del TEDH, que el 17 de octubre de 2019 consideró legítima la instalación de dichas cámaras al realizar el test de proporcionalidad: las cámaras se instalaron en lugares visibles y accesibles al público, la grabación se prolongó únicamente diez días y las imágenes fueron visionadas por un número limitado de personas. El TEDH estimó innecesaria la previa notificación de la instalación de las cámaras a los trabajadores por existir una «sospecha razonable» de incumplimiento grave de las obligaciones laborales.

Finalmente, el art. 89.3 LOPDGDD resulta especialmente restrictivo ante la utilización de dispositivos de grabación de sonidos por considerarlos especialmente invasivos en la intimidad de los trabajadores: no solo excluye la legitimidad empresarial fundada exclusivamente en el control de las obligaciones laborales de los trabajadores, sino que la restringe a los supuestos en que se pone en riesgo la seguridad de bienes y personas. Además, adiciona limitaciones derivadas del principio de proporcionalidad o de intervención mínima —acompañadas, obviamente, por las exigencias de información previa— y plazos específicos para la supresión [39].

VIII. LA VULNERABILIDAD DIGITAL

Existen grupos sociales especialmente amenazados o necesitados de una acción tuitiva de los poderes públicos para preservar su dignidad y libre desenvolvimiento en el mundo digital. Como acabamos de constatar, la exigencia de igualdad de oportunidades se proyecta singularmente en la necesidad de superar las brechas digitales de género, rurales y generacionales. Por tanto, las personas con discapacidad o necesidades especiales requieren del impulso de políticas específicas.

[39] Estas previsiones legales constituyen un marco mínimo de protección de los trabajadores que podrá ser ampliado en el marco de la negociación colectiva. El art. 91 («Derechos digitales en la negociación colectiva») resalta que «los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral».

Sin embargo, la vulnerabilidad digital resulta especialmente sensible y adquiere un especial significado y atención en niños o jóvenes. La toma de conciencia de esta realidad ha resultado inequívoca en los últimos años y se han adoptado estrategias dirigidas a su protección, pero estas resultan aún insuficientes (Pérez Álvarez *et al.*, 2014; Davara Fernández de Marcos, 2017)[40]. Desde el primer momento, el legislador europeo fue plenamente consciente de la necesidad de otorgar especial protección a los menores ante las agresivas estrategias de los proveedores de servicios de internet, que no se acompañaban de instrumentos efectivos dirigidos a que jóvenes y menores accedieran a dichos servicios a partir del momento en que gozaran de la madurez necesaria para tener suficiente conciencia de sus decisiones y riesgos. Una paradigmática manifestación de la preocupación del legislador ante la profusa difusión de informaciones personales de menores en las redes sociales y de los perjuicios futuros que pudiera causarles con el paso del tiempo y, en su caso, alcanzada la mayoría de edad, la encontramos en el art. 94.3 LOPDGDD («Derecho al olvido en servicios de redes sociales y servicios equivalentes») al consagrar el derecho de «toda persona» (menor o mayor de edad) a suprimir «a su simple solicitud» (sin necesidad de justificación alguna y de forma inmediata) los datos personales que se hubiesen facilitado, por él o por terceros, para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes «durante su minoría de edad». Una previsión legal que alcanza su pleno significado en la voluntad del legislador europeo manifestada en el considerando 65 del RGPD cuando afirma: «Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido". [...] Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño».

Los menores de edad resultan especialmente vulnerables ante la realidad digital. Sin necesidad de recurrir a estudios estadísticos, resulta evidente que la utilización de dispositivos digitales por menores de edad constituye una realidad generalizada, presidida por una utilización compulsiva que no ha sido posible minimizar a través de los mecanismos de control parental que facilitan los proveedores de servicios. La inmadurez social inherente a la

[40] La norma más reciente dirigida a tal fin ha sido el RGPD cuyo considerando 38 establece: «Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales».

minoría de edad convierte en reales los riesgos y amenazas que acechan tras el uso de la tecnología (Gargallo, 2017). El dilema existente entre las virtudes y los peligros que amenazan a los menores en el uso interno y externo de la tecnología únicamente puede resolverse apelando a la acción decidida de los progenitores y del sistema educativo. A los progenitores corresponde, como recuerda el art. 84.1 LOPDGDD, la tutela sobre el buen uso de la tecnología por sus hijos y, por ello, deben procurar «que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales». Un uso abusivo de la tecnología por los menores afecta a sus pautas de comportamiento personal y su modelo de relaciones sociales y altera un adecuado modelo de desarrollo de su personalidad. La función parental de los progenitores resulta decisiva en la aproximación de los menores al uso de la tecnología, pero no es suficiente (Rodríguez *et al.*, 2018). El sistema educativo no puede seguir ajeno a su función orientadora y formadora, como ya hemos advertido: el derecho a la educación digital debe posibilitar un sistema educativo comprometido con la tutela digital de los menores alejando sus riesgos, especialmente en ámbitos especialmente sensibles como el acceso a las redes sociales y servicios de internet (Rallo Lombarte, 2013)[41].

Establecer límites temporales en el otorgamiento del consentimiento de los menores de edad para facilitar sus datos personales, como establece el art. 8 RGPD, constituye el elemento garantista axial, pues implica imponer reglas cuyo cumplimiento resultará inexcusable para los proveedores de servicios de internet. Pero no solo. Este precepto no solo impone que el tratamiento de los datos personales de un niño en las ofertas directas de los servicios de la sociedad de la información solo se considerará lícito cuando los facilite directamente a partir de los 16 años o, por debajo de ese umbral, cuando el

[41] El art. 84.2 establece que la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor. No resulta gratuita esta específica referencia a la difusión de imágenes e información personal en redes sociales. La compulsiva difusión de información personal (particularmente, imágenes a través de fotos y vídeos) por los menores de edad en redes sociales constituye un fenómeno tan merecedor de reflexión como de preocupación por los riesgos que comporta como sustrato sobre el que se desarrollan numerosas conductas delictivas o, sin más, se vulneran derechos fundamentales (y, en particular, el derecho a la protección de datos de terceros).

consentimiento lo otorgue el titular de la patria potestad. La experiencia ha evidenciado que numerosos servicios de internet burlaban la esencia de estas genéricas obligaciones legales que imponían un determinado rango de edad para facilitar lícitamente datos personales al no incorporar efectivos sistemas que garantizaran su cumplimiento efectivo. Por ello este precepto, tomando como referencia el modelo establecido en el reglamento español de desarrollo de la LOPD, impone a los responsables de los servicios de internet el deber de cometer esfuerzos razonables para verificar la validez de este consentimiento atendiendo a la tecnología disponible.

Ahora bien, el legislador europeo no fue ajeno a la asimetría existente en los Estados miembros de la Unión Europea sobre las capacidades de autodeterminación jurídica de los menores de edad. Por ello, el RGPD atribuyó a los Estados miembros la capacidad para establecer por ley una edad inferior para prestar su autorización para la utilización de datos personales, aunque con el límite de los trece años. Y el legislador español —al igual que la mayoría de los Estados miembros— hizo uso de tal facultad rebajando la edad necesaria para otorgar tal consentimiento de los menores de edad a los catorce años (art. 7 LOPDGDD).

IX. LA MUERTE DIGITAL: ¿CAMBIO DE PARADIGMA EN LA PRIVACIDAD?

Han bastado apenas tres décadas de existencia de internet para constatar su enorme impacto no solo en la vida cotidiana de sus usuarios, sino también tras su fallecimiento. El uso profuso por los usuarios de numerosos servicios de internet que almacenan contenidos imbricados en la intimidad personal (servicios de mensajería, redes de relaciones personales, etc.) advierte de una acumulación de información personal que, caso de acceso por terceros a la totalidad de estos contenidos por fallecimiento del usuario, permite una intromisión en su intimidad de dimensiones inimaginables en el pasado: toda una vida de conversaciones privadas mantenidas a través de los servicios de mensajería o las relaciones personales más íntimas mantenidas durante décadas a través de redes sociales o servicios equivalentes desnudarían ante terceros toda una existencia personal que, en vida, estaría amparada por el secreto de las comunicaciones, la intimidad personal o la protección de los datos personales.

Pero, entre los retos actuales que se ciernen sobre el devenir de internet, nos encontramos con el de dar respuesta al destino que debe darse a la información personal acumulada en sus muy diferentes servicios por los usuarios tras su fallecimiento. A falta de una regulación específica, los prestadores de servicios de internet venían proporcionado a los usuarios la facultad de decidir

en vida el destino de su información personal, pero lo cierto es que las estadísticas evidencian el escasísimo uso de tal facultad por no estimarlo prioritario el usuario o por no facilitársele una fácil activación de este mecanismo por los proveedores de servicios. Por estos motivos, el art. 96 LOPDGDD consagra el «derecho al testamento digital» como el derecho de toda persona fallecida a decidir sobre el destino de los contenidos gestionados por prestadores de servicios de la sociedad de la información y a prohibir el acceso a los mismos de terceros impidiéndoles resolver sobre su utilización, destino o supresión, exceptuándose el derecho de los herederos a acceder a contenidos integrados en el caudal relicto. Por defecto, a falta de dicha prohibición, este precepto habilita a las personas vinculadas al fallecido por razones familiares o de hecho, así como a sus herederos, a dirigirse a los prestadores de servicios de la sociedad de la información para acceder a dichos contenidos e impartir las instrucciones que estimen oportunas sobre su utilización, destino o supresión. En particular, este precepto faculta para decidir sobre el mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia.

La razonabilidad de esta novedosa regulación esta fuera de duda si imaginamos el supuesto que la inspira: la automatizada interacción de relaciones personales protagonizada por un usuario fallecido en redes sociales obligaría a familiares y allegados a revivir el doloroso hecho luctuoso o, por ejemplo, numerosos usuarios vinculados al fallecido por internet desconocerían su muerte si terceros no tuvieran la capacidad de reaccionar y, cuanto menos, poner en conocimiento e instruir al servicio de internet sobre el destino del perfil personal en la red social o en los numerosos servicios equivalentes existentes. Sin embargo, este precepto ha planteado interrogantes sobre el alcance de la intromisión en la privacidad de una persona fallecida derivada del acceso a contenidos digitales de terceros. La mayoría de los prestadores de servicios de internet ya contemplan la posibilidad de que los usuarios de redes sociales decidan sobre el destino de sus contenidos en caso de fallecimiento, pero el uso de esta facultad es marginal. Facultar en exclusiva a los usuarios a decidir en vida sobre el destino de sus contenidos digitales supondría *de facto* impedir a terceros dicho acceso y residenciar en exclusiva en los responsables de estos servicios la capacidad de resolver sobre qué hacer con los contenidos digitales de un usuario fallecido. Por ello, el art. 96 LOPDGDD invierte la regla general al facultar a un elenco de personas legitimadas por vínculos familiares, jurídicos o *de facto*, a acceder a dichos contenidos y resolver sobre su destino.

Se ha suscitado, además, un sugerente debate sobre si el acceso de terceros a los contenidos digitales de una persona fallecida puede considerarse una intromisión excesiva en su privacidad. Esta cuestión nos traslada al recurrente

debate sobre el cambio de paradigma en el significado de la privacidad provocado por la revolución tecnológica. A medida que parece banalizarse el valor de la privacidad en la era digital, se adquiere más conciencia del impacto extraordinario que en la privacidad del individuo, en vida o fallecido, puede provocar un acceso total al conjunto de contenidos digitales que haya proporcionado y almacenado a lo largo de toda su vida en redes sociales, servicios de mensajería, etc. Esta progresiva toma de conciencia obligará a los proveedores de servicios de internet a procurar alternativas que minimicen estos temores (fechas de caducidad automática de la información, compartimentación de los contenidos, etc.).

Debe advertirse, por si restara alguna duda, que la persona fallecida ya no es titular del derecho fundamental a la protección de datos personales y, en consecuencia, nadie podrá predicar sobre sus datos los derechos y principios que inspiran la legislación de protección de datos. Cualquier actuación sobre su información personal deberá encontrar amparo en normativa adicional y específica que, en el supuesto que nos ocupa, reside en el art. 3 LOPDGDD. De forma que los dos preceptos referidos facultan, en sus propios términos, a terceros a decidir sobre el destino de contenidos —conservados en cualquier formato de almacenamiento o, específicamnete, en redes sociales o servicios equivalentes— que ya no son, en puridad, datos personales. Pero esta modificación de estatuto jurídico en la información vinculada a una persona fallecida arrumba las garantías proporcionadas por el dereho fundamental a la protección de datos personales, aunque ampara la tutela reconocida constitucionalmente del derecho fundamental a la intimidad de un fallecido por parte de sus allegados.

¿Cuál es el límite en la intromisión por parte de sus allegados (familiares, herederos, personas vinculadas afectivamente, etc.) de la intimidad de un fallecido? A falta de disposición expresa contraria del fallecido y en supuesto de conflicto que obligue a fijar la prelación entre los sujetos referidos en los arts. 3 y 96 LOPDGDD, parece razonable afirmar que únicamente a quienes el fallecido haya otorgado la condición de herederos (o, a falta de declaración testamentaria expresa, a quienes el ordenamiento jurídico otorgue tan legítima condición) correspoderá la facultad de conocer y decidir sobre el destino de cualesquiera información o contenidos obrantes en internet. Entendiendo que el acto de última voluntad de una persona en el que identifica a sus herederos constituye la manifestación inequívoca de un vínculo personal que trasciende la dimensión económica y alcanza cualesquiera otra dimensión privada.

X. CONCLUSIONES

La LO 3/2018 constituye un salto cualitativo en la necesidad de garantizar en la sociedad digital contemporánea derechos que garanticen la subordinación de la tecnología al individuo y que preserven su dignidad en la totalidad de ámbitos en que las personas actúan en sociedad. Los nuevos derechos digitales incluidos en su título X permiten verificar la necesidad de trasladar la garantía efectiva de los derechos constitucionales al mundo virtual, adaptándolos a las singularidades de la realidad *online*.

Esta elevación a rango legal de un catálogo de derechos digitales plantea numerosos interrogantes y reflexiones sobre su anclaje constitucional y sobre el expreso mandato constituyente para su desarrollo. Quedan zonas de penumbra que este desarrollo legislativo no puede resolver, a la espera de acciones positivas de los poderes públicos y de procesos aplicativos jurisprudenciales que concilien su colisión con otros derechos y libertades y demuestren su garantía efectiva.

Garantizar derechos digitales no implica únicamente procurar que los ciudadanos no vean limitada su capacidad de uso de la tecnología o preservar que los individuos puedan hacer valer sus derechos frente a la tecnología. La garantía efectiva de los derechos en la era digital impone obligaciones a los poderes públicos para posibilitar un acceso pleno a las herramientas tecnológicas que permita el desarrollo de su personalidad en el mundo digital contemporáneo.

Bibliografía

Alemán Páez, F. (2017). El derecho de desconexión digital. *Trabajo y Derecho,* 30, 12-33.

Alguacil González Aurioles, J. (2001). La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000). *Teoría y Realidad Constitucional*, 7, 365-385. Disponible en: https://doi.org/10.5944/trc.7.2001.6543.

Aragüez Valenzuela, L. (2017). El impacto de las tecnologías de la información y la comunicación en la salud de los trabajadores: el tecnoestrés. *e-Revista Internacional de la Protección Social*, 2 (2), 169-190. Disponible en: https://doi.org/10.12795/e-RIPS.2017.i02.12.

Barata, J. (2012). El concepto de net neutrality y la tensión entre regulación pública y autorregulación privada de las redes. *IDP Revista de Internet, Derecho y Política*, 13, 22-23.

Bárcena, J. M. (2016). Las transformaciones del derecho de la información en el contexto del ciberperiodismo. *Revista de Estudios Políticos*, 173, 141-168. Disponible en: https://doi.org/10.18042/cepc/rep.173.04.

Barrio Andrés, M. (2017a). *Fundamentos del derecho de internet*. Madrid: Centro de Estudios Políticos y Constitucionales.

—— (2017b). *Derecho público e internet: la actividad administrativa de regulación de la red*. Madrid: Instituto Nacional de Administraciones Públicas.

—— (2018). Los nuevos derechos digitales en España. *El País*, 24-12-2018. Disponible en: https://bit.ly/2GqN6GT.

—— (2019). La garantía de los derechos digitales en la LOPDGDD (Título X). En J. López Calvo (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 217-271). Madrid: Wolters Kluwer; Bosch.

Benito García, J. M. (2004). *La universalización del acceso a la información en el derecho de rectificación* [tesis doctoral]. Universidad Complutense. Disponible en: https://bit.ly/2TZnlpb.

Berners-Lee, T. (2010). Long live the web: a call for continued open standards and neutrality. *Scientific American*, 303 (6), 80-85. Disponible en: https://doi.org/10.1038/scientificamerican1210-80.

Cabeza Pereiro, J. (2018). El necesario cambio en la jurisprudencia constitucional sobre videovigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH. *Temas Laborales*, 141, 13-36.

Carrizosa Prieto, E. (2012). El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores. *Temas Laborales*, 116, 251-267.

Castaño, C. (dir.). (2008). *La segunda brecha digital (feminismos)*. Madrid: Cátedra.

Cialti, P. H. (2017). El derecho a la desconexión en Francia: ¿más de lo que parece? *Temas Laborales*, 137, 163-181.

Corredoira Alfonso, L. y Cotino Hueso, L. (dirs.). (2013). *Libertad de expresión e información en internet. Amenazas y protección de los derechos personales*. Madrid: Centro de Estudios Políticos y Constitucionales.

Cotino Hueso, L. (coord.). (2007). *Libertad en internet. La red y las libertades de expresión e información*. Valencia: Tirant lo Blanch.

—— (ed.). (2011). Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías. Valencia: Universidad de Valencia.

Davara Fernández de Marcos, L. (2016). *Implicaciones socio-jurídicas de las redes sociales*. Pamplona: Aranzadi. Disponible en: https://doi.org/10.2307/j.ctvrzgwjm.11.

—— (2017). *Menores en internet y redes sociales*. Madrid: Boletín Oficial del Estado.

Di Meo, R. (2017). Il diritto alla disconnessione nella prospettiva italiana e comparata. *Labour and Law Issues*, 3 (2), 17-38.

Fernández Esteban, M. L. (1999). La regulación de la libertad de expresión en internet en Estados Unidos y en la Unión Europea. *Revista de Estudios Políticos*, 103, 149-169.

Frosini, T. E. (2011). Il diritto costituzionale di acceso a internet. *AIC Rivista Telematica Giuridica dell´Associazione Italiana dei Costituzionalisti*, 2, 1-17.

García-Alonso Montoya, P. (2006). Periodismo digital y periodismo ciudadano. En *Análisis y propuestas en torno al periodismo digital. VII Congreso Nacional Periodismo Digital* (pp. 251-262). Huesca: Asociación de Prensa de Aragón.

García Mexía, P. (2005). *Principios de derecho de internet*. Valencia: Tirant lo Blanch.

—— (2009). *Derecho europeo de internet*. A Coruña: Netbiblo.

—— (2017). *La internet abierta. Retos regulatorios de una red nacida libre*. Madrid: REU Ediciones.

Gargallo, E. L. (2017). *La seguridad para los menores en internet*. Barcelona: Editorial UOC.

Gil Antón, A. M. (2012). El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales. *Revista de Derecho UNED*, 10, 209-255.

González San Juan, J. L. (2016). Neutralidad de red en internet. *Ibersid*, 10 (2), 39-44.

Goñi Sein, J. L. (2007). *La videovigilancia empresarial y la protección de datos personales*. Madrid: Thomson Civitas.

—— (2009). Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos. *Justicia Laboral: Revista de Derecho del Trabajo y de la Seguridad Social*, 2009, 11-58.

Gude Fernández, A. (2014). La videovigilancia en el ámbito laboral y el derecho a la intimidad. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 35, 109-134.

Guerrero Pico, M. C. (2005). El derecho fundamental a la protección de los datos de carácter personal en la Constitución europea. *Revista de Derecho Constitucional Europeo*, 4, 293-334.

Jiménez-Castellanos Ballesteros, I. (2017). Videovigilancia laboral y derecho fundamental a la protección de datos. *Temas Laborales*, 136, 129-156.

López Calvo, J. (coord.). (2017). *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Sepín.

—— (coord.). (2019). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid: Wolters Kluwer; Bosch.

López Ortega, J. J. (2001). Libertad de expresión y responsabilidad por los contenidos en internet. *Cuadernos de Derecho Judicial*, 10, 83-126.

Lucas Murillo de la Cueva, P. (1993). *Informática y protección de datos personales*. Madrid: Centro de Estudios Políticos y Constitucionales.

—— (2003). La primera jurisprudencia sobre el derecho a la autodeterminación informativa. *Datospersonales.org: la Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, 1, 9.

Manrique López, F. (2011). Los derechos fundamentales y la intimidad de los trabajadores: fórmulas de acceso y control. *Derecho y Nuevas Tecnologías*, 1, 169-182.

Marín Alonso, I. (2004). La facultad fiscalizadora del empresario sobre el uso del correo electrónico en la empresa: su limitación en base al derecho fundamental al secreto de las comunicaciones. *Temas Laborales*, 75, 95-122.

Molina Navarrete, C. (2017). Jornada laboral y tecnologías de la info-comunicación: «desconexión digital», garantía del derecho al descanso. *Temas Laborales*, 138, 249-283.

Nannipieri, L. (2015). *Profili costituzionali dell'accesso ad internet* [tesis doctoral]. Università di Pisa. Disponible en: https://bit.ly/2GsEZJW.

Naranjo Colorado, L. D. (2017). Vicisitudes del nuevo derecho a la desconexión digital. Un análisis desde la base del derecho laboral. *Saber, Ciencia y Libertad*, 12-2, 49-57. Disponible en: https://doi.org/10.18041/2382-3240/saber.2017v12n2.1531.

Naval Durán, C, Serrano Puche, J., Sádaba Chalezquer, C. y Arbués Radigales, E. (2016). Sobre la necesidad de desconectar: algunos datos y propuestas. *Education in the Knowledge Society (EKS)*, 17 (2), 73-90. Disponible en: https://doi.org/10.14201/eks20161727390.

Pérez Álvarez, S., Burguera Ameave, L. y Paul Larrañaga, K. (dirs.). (2014). *Menores e internet*. Pamplona: Aranzadi.

Pérez Luño, A. E. (2012). *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas. Disponible en: https://doi.org/10.5209/rev_ANDH.2011.v12.38107.

Pérez Martínez, J. (coord.). (2011). *Neutralidad de Red: aportaciones al debate*. Barcelona: Ariel; Fundación Telefónica.

Pisa, R. (2010). L´accesso ad internet: un nuovo diritto fondamentale? *Enciclopedia Treccani*, 7. Disponible en: https://bit.ly/2ONXrlD.

Quílez Moreno, J. M. (2018). Conciliación laboral en el mundo de las TIC. Desconectando digitalmente. *Revista General de Derecho del Trabajo y de la Seguridad Social,* 51, 305-324.

Rallo Lombarte, A. (2013). La protección de la privacidad en las redes sociales de internet: la experiencia canadiense con Facebook. En A. Rallo y R. Martínez (eds.). *Derecho y Redes sociales* (pp. 257-284). Pamplona: Civitas-Thomson Reuters.

—— (2014). *El derecho al olvido en internet. Google versus España*. Madrid: Centro de Estudios Políticos y Constitucionales.

—— (2017a). De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, 100, 637-667.

—— (2017b). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet. *Teoría y Realidad Constitucional*, 39, 583-610. Disponible en: https://doi.org/10.5944/trc.39.2017.19150.

—— (2018a). Nuevas tecnologías, nuevos derechos. *España constitucional (1978-2018). Trayectorias y Perspectivas* (vol. 3) (pp. 2363-2379). Madrid: Centro de Estudios Políticos y Constitucionales.

—— (2018b). *The right to be forgotten on the internet: Google vs Spain*, Washington: Electronic Privacy Information Center.

—— (2019a). Del derecho a la protección de datos a la garantía de nuevos derechos digitales. En A. Rallo Lombarte (dir.). *Tratado de Protección de Datos* (pp. 23-52). Valencia: Tirant lo Blanch. Disponible en: https://doi.org/10.18042/cepc/redc.116.02.

—— (2019b). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, 116, 47-74. Disponible en: https://doi.org/10.18042/cepc/redc.116.02.

—— y García Mahamut, R. (eds.). (2015). *Hacia un nuevo derecho europeo de protección de datos. Towards a new European Data Protection Regime*. Valencia: Tirant lo Blanch.

—— y Martínez, R. (2013a). Data Protection, Social Networks, and Online Mass Media. En S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (eds.). *European Data Protection: Coming of Age* (pp. 407-423). London; New York: Springer. Disponible en: https://doi.org/10.1007/978-94-007-5170-5_19.

—— y Martínez, R. (eds.). (2013b). *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters.

Rodríguez Cardo, I. A. (2014). Política empresarial previa y supresión de la expectativa de privacidad: una reflexión crítica sobre las facultades control del ordenador utilizado por el trabajador. *Temas Laborales*, 126, 167-197.

Rodríguez Escanciano, S. (2015). *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*. Valencia: Tirant lo Blanch.

Rodríguez, P., Martín, S. y Blanco, J. C. (2018). *Familias enREDadadas. Los riesgos en internet*. Madrid: Morata.

Ruiz Miguel, C. (2003). El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico. *Revista de Derecho Comunitario Europeo*, 14, 7-43.

Sáez Lara, C. (2017). Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y de la comunicación. *Temas Laborales*, 138, 185-221.

Taléns Visconti, E. E. (2018). La desconexión digital en el ámbito laboral. Un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva. *Revista de Información Laboral,* 4, 193-208.

Troncoso Reigada, A. (2010). *La protección de datos personales en busca del equilibrio*. Valencia: Tirant lo Blanch.

Vallecillo Gámez, M. R. (2017). El derecho a la desconexión ¿«Novedad digital» o esnobismo del «viejo» derecho al descanso? *Estudios Financieros. Revista de Trabajo y Seguridad Social*, 408, 167-178.

Villaverde Menéndez, I. (1994). Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993. *Revista Española de Derecho Constitucional,* 41, 187-224.

Zolo, D. (2009). Nuovi diritti e globalizzazioni. *Enciclopedia Treccani*. Disponible en: https://bit.ly/32nXCs4.