MONOGRAFÍAS

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA SOCIEDAD DIGITAL

Mª Emilia Casas Baamonde Coordinadora
Juan Luis Requejo Pagés | José Luis Piñar Mañas
Mercedes Pérez Manzano | Ignacio García-Perrote Escartín

FUNDACIÓN
RAMÓN ARECES

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA SOCIEDAD DIGITAL

Mª Emilia Casas Baamonde Coordinadora

MONOGRAFÍAS

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA SOCIEDAD DIGITAL

Mª Emilia Casas Baamonde Coordinadora

Juan Luis Requejo Pagés Letrado del Tribunal de Justicia de la Unión Europea

José Luis Piñar Mañas Catedrático de Derecho Administrativo. Universidad CEU-San Pablo de Madrid

Mercedes Pérez Manzano Catedrática de Derecho Penal, Universidad Autónoma de Madrid

Ignacio García-Perrote Escartín Catedrático de Derecho del Trabajo (UNED)

FUNDACIÓN
RAMÓN ARECES

EDICIÓN 2020

Tomás Bretón, 21 - 28045 Madrid
T 915 398 659
F 914 681 952
cerasa@cerasa.es
www.cerasa.es

Vitruvio, 5 - 28006 Madrid
www.fundacionareces.es

Diseño:
KEN | www.ken.es

Depósito legal: M-13538-2020

Impreso por:

ANEBRI, S.A.
Antonio González Porras, 35-37
28019 Madrid
Impreso en España | Printed in Spain

ÍNDICE

PRESENTACIÓN

Los ensayos que recoge esta Monografía se corresponden con el ciclo de conferencias organizado por la Fundación Ramón Areces sobre «El derecho a la protección de datos personales en la sociedad digital», impartidas en la primavera y primeros día del verano de 2019 por cuatro destacados especialistas del tratamiento normativo de estos derechos, todos ellos profesores e investigadores universitarios, aunque también en todos hayan concurrido o concurran otros reconocidos ejercicios profesionales: Juan Luis Requejo Pagés, José Luis Piñar Mañas, Mercedes Pérez Manzano e Ignacio García-Perrote Escartín. Sus aportaciones han desentrañado y valorado la adecuación de las garantías levantadas en defensa del derecho a la protección de datos personales por la Constitución, el Derecho de la Unión Europea, la citada Ley Orgánica 3/2018, de 5 de diciembre, el sistema jurídico penal y la legislación laboral.

La Fundación Ramón Areces ha querido contribuir a profundizar y especializar la reflexión de la mano de indiscutibles expertos jurídicos de distintas especialidades para conocer y difundir las razones de la necesidad de la protección por el sistema jurídico de los datos personales, de la realidad de esa protección ante la imparable innovación tecnológica y de sus retos y desafíos, de la eficacia de las garantías jurídicas y de sus límites.

Como el lector comprobará, los autores no han esquivado ninguna cuestión polémica y se han adentrado con pleno dominio en sus respectivos campos de análisis. En todos ellos aparecen preocupaciones comunes como la intervención humana en el control de la tecnología o la humanización de la tecnología, la eficacia del Derecho y de sus instrumentos de tutela ante transformaciones tecnológicas tan veloces e imparables, siempre de alcance global. Y todos coinciden en una propuesta común: la defensa de los derechos fundamentales, y en concreto del derecho fundamental a la protección de datos de carácter personal, que son el fundamento de la democracia, y de la persona, que lo es de los derechos y del Estado constitucional. Sin privacidad y libertad de las personas no hay democracia y esa ley principal de ordenación política debe regir el mundo de internet, el universo digital.

Sólo me queda recomendar la lectura de esta excelente Monografía y desear el éxito de las propuestas de sus autores, lo que hago vivamente.

María Emilia Casas Baamonde
Consejo de Ciencias Sociales Fundación Ramón Areces

1

INTRODUCCIÓN

MARÍA EMILIA CASAS BAAMONDE
Consejo de Ciencias Sociales Fundación Ramón Areces

La utilización de las nuevas tecnologías digitales genera grandes cantidades de datos relativos a las personas usuarias, cuyo conocimiento y tratamiento plantean riesgos evidentes para sus derechos y libertades, en concreto para sus derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de datos personales y, por tanto, para los sistemas constitucionales democráticos en las sociedades digitalizadas, incluida nuestra Constitución, que reconoce y tutela esos derechos fundamentales.

El «poder» de los datos mueve el mundo en que vivimos. La información obtenida sobre los comportamientos de las personas usuarias de los servicios de la sociedad de la información son convertidos en datos por las grandes plataformas digitales de gestión masiva de esos datos y en ingentes beneficios económicos. Afecta a todos los ámbitos en que se desenvuelve la vida de las personas sin excepción, marcada por las oportunidades abiertas por las tecnologías digitales y, al tiempo, por la amenaza que suponen para nuestros datos personales.

Los datos valen en cuanto circulan y son tratados y permiten formular pronósticos de comportamiento de las personas provechosos para infinidad de actividades económicas y sociales. Se han convertido en materia prima esencial del mercado y en elemento determinante de la toma de decisiones de diversa naturaleza que nos afectan, o pueden hacerlo decisivamente, pero trascienden nuestra volición y ámbito de autonomía personal.

El derecho de las personas a la protección de sus datos se traduce en un poder jurídico de disposición y control sobre los propios datos frente a terceros, Estados y particulares. Se enfrenta a un reto infinitamente mas complejo y alarmante del que creíamos cuando el derecho se reconoció como libertad informática o libertad frente a la informática, ante el flujo incesante y creciente de informaciones, conexiones u operaciones en la Red, que franquean el acceso de terceros al conocimiento de datos personales, inadvertidamente en ocasiones por sus titulares, y a su posterior almacenamiento, tratamiento y uso por quienes los han obtenido.

El derecho de control sobre los datos relativos a la propia persona, que es también un derecho de oposición a su utilización por otros, puede desfallecer al compás de las experiencias de los usuarios en operaciones virtuales en masa en el mundo de internet que crecen a velocidad de vértigo. Por ello el contenido y el despliegue funcional de este derecho fundamental demanda una atención permanente en garantía de su efectividad.

La Unión Europea y los Estados han puesto en marcha políticas de protección para que las personas mantengan el poder de control sobre sus datos personales, sobre su posesión, uso y destino, que los poderes públicos y las entidades privadas han de respetar. La Ley Orgánica 3/2018, de 5 de diciembre, ha adaptado a nuestro Derecho el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, «relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos» (Reglamento general de protección de datos) y, además, ha incluido en su regulación los que denomina derechos digitales en relación con internet, las redes sociales u otros dispositivos digitales.

No podían los legisladores europeo e interno permanecer impávidos ante los riesgos que para la privacidad y libertad de las personas proceden del entorno tecnológico, no obstante las dificultades de enfrentar un fenómeno transnacional en el espacio público mundial en el que actúan las plataformas digitales de tratamiento y gestión de datos de difícil control por el poder de los Estados y de la propia Unión Europea al tener su sede fuera del territorio europeo. El Derecho, incluido el de los tribunales, ha de ofrecer soluciones frente a fenómenos que han cambiado la marcha del mundo, la irrupción de nuevos sujetos de poder y la eclosión de nuevos cánones, o la desaparición de los que dábamos por establecidos, lo que no es sino el signo obligado de su supervivencia y de la efectividad de sus técnicas diferenciadas de intervención social.

El derecho fundamental a la protección de los datos personales tiene el contenido esencial señalado, que se impone al legislador también en realidades tecnológicas especialmente complejas, sujetas a un gran dinamismo. Su desarrollo legislativo está hoy parcialmente determinado por el Derecho de la Unión Europea, cuyas exigencias, ha dicho el Tribunal Constitucional, «no pueden ser irrelevantes a la hora de establecer los márgenes constitucionalmente admisibles de la libertad de apreciación política» (Sentencia 76/2019, de 22 de mayo, FJ 3). Por ello su regulación jurídica, estructuralmente compleja, ha suscitado numerosos análisis y debates.

Los textos son, obviamente, hijos de su tiempo. En el transcurrido entre la impartición de las conferencias y la publicación de esta monografía el cambio más relevante que hemos vivido, sin parangón posible, ha sido la inédita y terrible situación de emergencia sanitaria causada por la asoladora pandemia de COVID-19, iniciada en la ciudad china de Wuham en diciembre de 2019. El Gobierno decretó el estado constitucional de alarma el 14 de marzo de 2020, restringiendo nuestros derechos y libertades constitucionales, especialmente de circulación y residencia, de actividad empresarial y de trabajo, para contener la expansión del virus y sus efectos de enfermedad y letalidad en la población. En una situación tan extrema las tecnologías digitales han mostrado su capacidad y han permitido la continuidad de la actividad de millones de personas e instituciones en nuestro país y en el mundo. El teletrabajo ha tenido un crecimiento exponencial. El régimen jurídico del tratamiento de datos personales especiales o especialmente protegidos, los relativos a la salud naturalmente, ha quedado afectado, no por el decreto de declaración del estado excepcional de alarma, sino por las limitaciones contempladas en su propia normativa, que posibilita el tratamiento lícito de esos datos por las autoridades sanitarias y por los empleadores en el ámbito de su responsabilidad de prevención de riesgos para la salud de los trabajadores en el trabajo, en la satisfacción del interés esencial de la vida de las personas y de la salud pública con la debida proporcionalidad para

la salvaguarda de esos intereses y para la preservación de la esencialidad del derecho fundamental. Las legislaciones de salud pública y de prevención de riesgos laborales en el trabajo complementan las limitaciones de la regulación legal del derecho autónomo a la protección de los datos personales.

Esta monografía no ha podido ocuparse de esta extraordinaria situación, pero el lector encontrará en ella, en los análisis precisos, críticos y siempre sólidamente argumentados de sus autores, las claves de comprensión del ámbito operativo del derecho a la protección de los datos personales y de sus limitaciones legales, estas especialmente consideradas por razones de la persecución de delitos o de control empresarial del trabajo. En la cotidianidad de la vida y en la excepcionalidad de la emergencia sanitaria, el de la protección jurídica de los datos personales es uno de los grandes temas de las sociedades democráticas, tratado con la convicción común, abiertamente declarada por los autores, de que en la realidad del derecho determinada por la Constitución se encuentra su comprensión cabal. Y, en consecuencia, el punto de partida de los análisis.

LA CONSTITUCIÓN Y EL DERECHO DE LA UNIÓN EUROPEA

Proverbial es la capacidad del profesor Juan Luis Requejo Pagés de situar con precisión los temas que trata. Aquí, la que denomina encrucijada en que se encuentra la protección de datos entre el Derecho de la Unión Europea y la Constitución española, encrucijada en la que se decide el camino del proceso de integración europea hacia una verdadera Unión de Estados o hacia la vuelta a los Estados nacionales y la suerte de los derechos fundamentales reconocidos por las Constituciones nacionales. En esa encrucijada reflexiona el autor sobre el precio que el Derecho de la Unión puede cobrarse en los derechos fundamentales a la intimidad y a la protección de datos, señaladamente en este último derecho definido por el Tribunal Constitucional (Sentencia 292/2000, de 30 de noviembre) como un derecho autónomo que, como ya he dicho, en síntesis se sustancia en el poder de disposición de la persona sobre sus datos, y que el Tribunal Constitucional encuadró en el espacio abierto por el artículo 18, apartado 4, de la Constitución, que ha establecido «una tímida garantía» normativa de los derechos fundamentales al honor, a la intimidad, y a la propia imagen de las personas, «frente a una revolución todavía por venir».

Es rotundo el profesor Requejo: «El problema de fondo planteado por el tratamiento de los datos personales es esencialmente el problema de la libertad»; se «cierne [...] sobre el individuo un poder de una fuerza formidable, capaz de condicionar su conducta de manera imperceptible y, sobre todo, de definir las circunstancias de su ámbito vital hasta el punto de comprometer la autonomía necesaria para el ejercicio de la libertad». La elaboración de perfiles de las personas físicas, que permiten identificarlas tras el tratamiento automatizado de los datos dejados en su utilización de internet, es ejemplo expresivo de ese poder formidable. Esos «perfiles», en la regulación del Reglamento general de protección de datos y de la ley española, sirven en particular nada menos que «para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». Coherentemente, Requejo califica de cometido más urgente del constitucionalismo en las próximas décadas «la sujeción de los actores del universo digital», de los «poderes digitales», con un poder sobre la vida y la libertad de las

personas que rivaliza y puede superar al de los Estados, encorsetados en unos instrumentos de acción limitados.

El profesor Requejo muestra su inquietud ante la incapacidad del Derecho para adoptar una estrategia efectiva de defensa del derecho de libre disposición sobre los datos personales frente a las grandes plataformas tecnológicas, que obtienen información del tratamiento de los datos. El Reglamento general de protección de datos efectúa un encomiable esfuerzo de aplicación de sus normas mas allá del territorio de la Unión Europea, pues no importa que la plataforma esté establecida fuera de la Unión, ni que el tratamiento de los datos tenga lugar o no en la Unión. El problema es, con todo, que dicho Reglamento no se limita a procurar la protección de los datos personales, en línea con nuestra Constitución, sino a garantizar su libre circulación como libertad «comunitaria» fundamental, lo que exige que el «nivel» de protección del derecho de protección de datos sea equivalente en todos los Estados miembros para hacer realidad la libre circulación de los datos en la Unión y el buen funcionamiento del mercado interior. La dualidad de objetivos del Reglamento, la protección de las personas físicas frente al tratamiento de los datos personales y la libre circulación de esos datos, lleva al autor a proclamar que el logro de este segundo objetivo no puede ser restringido o prohibido por el primero.

La lógica inapelable del principio de primacía podría arriesgar el contenido del derecho fundamental de protección de datos en nuestra Constitución para conducirle a un nivel de protección más bajo, se teme Requejo. No es una previsión infundada si se tiene en cuenta que el legislador español ha decidido que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejerza con arreglo a lo establecido en el Reglamento general de protección de datos y a la ley orgánica.

A la vista de deciciones como la Sentencia de 13 de mayo de 2014, C-131/12, *Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González*, Requejo confía en que el Tribunal de Justicia inocule en la interpretación del artículo 8 de la Carta de los derechos fundamentales de la Unión Europea, que reconoce como tal el derecho a la protección de datos de carácter personal, el espíritu y la técnica de los derechos fundamentales, y no de las libertades del mercado.

¿REFORMAR LA CONSTITUCIÓN? DERECHO, TÉCNICA Y ÉTICA

La relación entre el Derecho de la Unión, el Reglamento general de protección de datos y la Constitución prosigue en el certero análisis del profesor José Luis Piñar Mañas que, al hilo de la Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, destaca la condición de la ley europea de «parámetro interpretativo del alcance y contenido» del derecho fundamental a la protección de datos personales reconocido en el art. 18.4 de la Constitución.

El profesor Piñar se pregunta si es necesario, en particular, reformar la Constitución, en la línea de la exposición de motivos de la Ley Orgánica 3/2018, para otorgar efectividad a los derechos en la sociedad digital *y qué cambios, en general, ha de adoptar el Derecho* para proteger la privacidad de las personas y sus datos personales ante el imparable avance tecnológico. Partiendo de que la Constitución admite una interpretación extensiva de sus derechos, valores y principios al entorno digital, no deja de resaltar los riesgos a que se enfrentan en ese entorno los derechos a la privacidad y a la identidad ante el tratamiento masivo de los datos personales. El derecho

a la identidad, entendido como derecho «a ser uno mismo y diferente de los demás», no reconocido como tal por la Constitución, enlazaría con la dignidad personal y el libre desarrollo de la personalidad, fundamento de los derechos. La identidad, «cualidad principal de la persona humana», en definición de la Sentencia del Tribunal Constitucional 99/2019, de 18 de julio, que configura y condiciona la propia vida, puede devenir en «una identidad controlada, diseñada y vigilada» producto de su «heteroformación» por el poder de los algoritmos. La elaboración de los perfiles puede configurar una identidad «desde fuera» que se vuelva contra la propia identidad, la personalidad del ser humano y su libre desarrollo. La persona debe poder controlar su identidad digital frente a la actuación de las grandes empresas multinacionales que basan en el tratamiento de datos gran parte de su actividad (Google, Facebook, Amazon, Microsoft, Linkedin, Yahoo, y tantas otras).

El profesor Piñar propone el diálogo, el «trílogo» entre el Derecho, la Técnica y la Ética para afrontar la innovación, y el retorno a un Derecho principal (principios de licitud, de lealtad, de responsabilidad proactiva, de transparencia, de limitación de la finalidad, de exactitud y de minimización) frente a la inevitable obsolescencia de unas soluciones normativas apegadas a una realidad concreta. La autorregulación estaría llamada a ejercer un papel principal en la regulación de la innovación tecnológica (códigos de conducta, códigos tipo, códigos deontológicos, normas corporativas vinculantes...). Esas técnicas contribuirían a la actualización y esclarecimiento de la regulación del derecho a la protección de datos personales, «de su contenido y alcance en la sociedad digital», pero también del derecho de acceso a internet, habilitante del acceso al ejercicio de otros múltiples derechos (de las libertades de circulación, expresión e información, de los derechos a la educación y a la cultura, a la justicia y a la defensa), y del derecho al conocimiento en general y al científico en particular, al menos al obtenido con financiación pública, pese a sus posibles colisiones con los derechos de propiedad intelectual.

La rica aportación del profesor Piñar no se queda aquí, sino que se adentra en el análisis de los derechos digitales o derechos de la ciudadanía digital y en la operación del legislador español de dar «anclaje» en el artículo 18.4 de la Constitución a la regulación de los derechos digitales, adicionando un nuevo título, el X, a la Ley Orgánica 3/2018. Crítico con esta opción legislativa, el profesor Piñar considera que la regulación de los derechos digitales hubieran debido merecer una ley orgánica propia que hiciera «honor a la importancia del tema».

Para el profesor Piñar los derechos fundamentales reconocidos para un mundo analógico han de tener su reflejo paralelo en el mundo digital bajo el presupuesto de que «la centralidad de la persona es clave de bóveda».

EL DERECHO A LA AUTODETERMINACIÓN INFORMÁTICA Y EL SISTEMA JURÍDICO PENAL

La profesora Mercedes Pérez Manzano aborda con su rigor característico los retos que el «derecho a la autodeterminación informática, o derecho al control de la publicidad de los datos personales», plantea al sistema penal. Su protección a través de las técnicas de prevención y sanción de las intromisiones ilegitimas de los particulares, tipificadas como delitos de descubrimiento y revelación de secretos, tiene una importancia innegable pero, al tiempo, los Estados precisan también del conocimiento de los datos personales para organizar políticas de persecución e in-

vestigación de los delitos. Esa finalidad justifica la legitimidad de la imposición de restricciones al derecho fundamental a la protección de los datos personales, y a los derechos fundamentales a la intimidad y al secreto de las comunicaciones.

El delito de allanamiento o intrusismo informático protege el derecho al control de la publicidad de cualesquiera tipo de datos, así «como los sistemas informáticos en sí mismos frente a las interferencias en el sistema». Frente a posiciones críticas, defiende la profesora Pérez Manzano la pertinencia y legitimidad de la intervención penal en la configuración de este delito, y su configuración autónoma, desvinculada de la protección de la intimidad y de la privacidad pese a su incorporación al grupo de los delitos contra la intimidad personal, por la relevante significación de los sistemas informáticos en la sociedad de la información, en la que «la integridad, confidencialidad, autenticidad (fiabilidad) y disponibilidad de los datos y de los sistemas informáticos son valores esenciales para garantizar el modelo actual de relaciones sociales, económicas y políticas». La confidencialidad, la integridad y la disponibilidad de los sistemas de información, sostiene la autora, constituyen una barrera de contención de riesgos para otros bienes jurídicos que se pueden ver involucrados en la función social de los sistemas informáticos (el patrimonio, la intimidad...).

No ahorra críticas, Pérez Manzano, a la tipificación del *hacking* informático en los delitos contra la intimidad (la exigencia de peligro para la intimidad personal en todo caso excluiría su aplicación a los casos de acceso a las infraestructuras críticas de los sistemas informáticos) con la perspectiva de los principios de legalidad (solapamientos de figuras delictivas y lagunas) y de proporcionalidad de las penas. La demanda de «reflexión sosegada», pese a la rapidez de las innovaciones, precede a la de modificaciones legislativas.

La necesaria unificación del régimen jurídico de la legitimidad de las restricciones impuestas a los derechos fundamentales a la intimidad informática y al secreto de las comunicaciones por razón de la investigación delictiva lleva a Pérez Manzano a exigir siempre autorización judicial individualizada para limitar los derechos vinculados con el entorno digital. La crítica a la jurisprudencia constitucional elaborada en los años 80 del pasado siglo para una realidad tecnológica bien diferente a la actual no podía hacerse esperar.

Tampoco la que dirige a las limitaciones del derecho a la protección de los datos personales fundadas en la investigación judicial en la regulación del Reglamento general de protección de datos y de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Reaparece aquí la doble lógica, no fácilmente cohonestable, del legislador europeo de proteger los datos personales y su libre circulación, advertida ya por el profesor Requejo, que la profesora Pérez Manzano enlaza con la lucha contra la criminalidad y su necesaria eficacia. En este sentido se queja de la amplitud y vaguedad con que se enuncian los fines legitimadores de las limitaciones del derecho a la protección de los datos personales en aras de ese objetivo (seguridad, interés público, protección de los derechos y libertades de otras personas, prevención, investigación, detección o enjuiciamiento de infracciones penales, ejecución de sanciones penales, protección y prevención frente a las amenazas contra la seguridad pública...), que los Estados podrán acoger. La consecuencia para el ciudadano es que «sea

casi imposible prever los casos en los que puede ver sus derechos limitados», sin necesidad de estar acusado y condenado, pues también los datos personales de las víctimas y testigos pueden resultar restringidos si su ejercicio supone «un obstáculo para las indagaciones».

El Tribunal de Justicia se ha ocupado, con el canon de proporcionalidad, del almacenamiento masivo de datos del tráfico de comunicaciones por proveedores de servicios de comunicaciones electrónicas y el acceso a los mismos por autoridades públicas, previamente autorizadas, por razones de investigación criminal (lucha contra la criminalidad grave, terrorismo, delincuencia organizada). Con ese canon de enjuiciamiento ha tratado la Corte europea de sostener una lógica garantista de los derechos.

Para evitar los efectos indeseados de construcción de un Derecho excepcionador de la protección de los datos personales («los peligros de ampliación del marco de las excepciones a la protección de los datos personales») cree la profesora Pérez Manzano que «urge la elaboración de una legislación europea mucho más precisa», «un reto, sin duda, asequible, pues contamos ya con un conjunto normativo de referencia muy amplio en materia de cooperación judicial penal en la Unión Europea».

LOS DERECHOS DE PRIVACIDAD EN LAS RELACIONES LABORALES

El profesor Ignacio García-Perrote ha efectuado una completa y fundada exploración y reflexión sobre el «impacto» del derecho a la protección de datos y de los derechos digitales en las relaciones laborales.

El control empresarial del uso por los trabajadores de los dispositivos digitales de la empresa plantea la doble problemática de determinar la licitud de las políticas internas empresariales prohibitivas del uso de esos dispositivos por las personas trabajadoras para fines privados, y de los medios de vigilancia, asimismo digitales, del uso prohibido. El conocimiento por los trabajadores, y la correspondiente obligación empresarial de información previa, de las instrucciones empresariales acerca de ese uso limitado a tareas profesionales y del modo de ejercicio del poder de supervisión empresarial de su cumplimiento es la clave de la conformación de la actuación empresarial a los derechos fundamentales de los trabajadores a la intimidad, al secreto de las comunicaciones, y a la protección de sus datos personales en el trabajo. Ni que decir tiene que esa supervisión, si es precisa para el cumplimiento de los objetivos empresariales, se sirve del acceso a los contenidos o datos derivados del uso de los dispositivos digitales empresariales. La información previa es por ello «absolutamente determinante». Con ser esto importante, no resuelve todos los problemas.

¿La ausencia de toda expectativa de confidencialidad del trabajador en el trabajo es compatible con la lógica de los derechos fundamentales? ¿Los criterios de utilización de los dispositivos digitales que establezcan los empresarios pueden anular la expectativa razonable de privacidad de los trabajadores? La Ley Orgánica 3/2018 ordena a los empleadores respetar «en todo caso los estándares mínimos de protección» de la intimidad de los trabajadores «de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente» (art. 87.3). Recuerda García-Perrote la advertencia de la Sentencia del Tribunal Europeo de Derechos Humanos, Gran Sala, de 5 de septiembre de 2017 (*Barbulescu II v. Rumanía*), de que las instrucciones empresariales «no pueden reducir a cero (o a la nada) la vida social privada en

los lugares de trabajo», y la consiguiente de que, en esos ámbitos, «el respeto de la vida privada y de la confidencialidad de la correspondencia (artículo 8 del Convenio Europeo de Derechos Humanos) sigue siendo necesario, aunque puede ser limitado en la medida en que ello sea necesario».

¿El deber de información previa de la política empresarial sobre el uso de los medios tecnológicos y de los mecanismos de control o vigilancia de ese uso forma parte del contenido esencial del derecho fundamental a la protección de datos del artículo 18.4 de la Constitución? ¿También frente a sospechas empresariales fundadas de la comisión de actos delictivos por los trabajadores en el trabajo, y en concreto a través de la utilización de los medios electrónicos empresariales?

Del conocimiento al consentimiento. Incide el profesor García-Perrote en la exigencia de consentimiento por la jurisdicción penal, de modo que un acceso inconsentido, o no autorizado judicialmente, al dispositivo de almacenamiento masivo de datos del trabajador para probar infracciones penales acarrea la contaminación de las pruebas.

El análisis del derecho a la desconexión digital frente a la conectividad excesiva, el protagonismo de las políticas internas empresariales, el papel de la negociación colectiva, el conocimiento del derecho comparado y exhaustivo de la jurisprudencia, constitucional y ordinaria, se dan la mano en el excelente trabajo de García-Perrote. No obstante las demandas contradictorias que el trabajo en la sociedad digitalizada ejerce sobre las personas, no es ilusorio contener la conectividad desmesurada y llevar la calidad de vida al trabajo, según propone la legislación francesa. Vuelve aquí el autor a dar cuenta del papel de las políticas internas empresariales, que no son otra cosa que políticas de actuación sobre el uso de los dispositivos tecnológicos, sobre las modalidades de ejercicio del derecho de desconexión digital y sobre el uso razonable de las herramientas tecnológicas para evitar el riesgo de fatiga informática, especialmente en las modalidades de trabajo a distancia a través del teletrabajo, extendido al limite de sus posibilidades por la gravísima crisis del coronavirus COVID-19.

El ejercicio de las funciones de control de los trabajadores a través de videovigilancia, con la consiguiente grabación de imágenes, o de sistemas de geolocalización, precisa igualmente de la información previa, expresa, clara y concisa a los trabajadores y, en su caso, a sus representantes. Ahora bien, si se ha captado la comisión flagrante de un acto ilícito por los trabajadores, o existen sospechas serias sobre esa comisión, se entiende cumplido el deber de informar cuando exista al menos el distintivo de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos. De no admitirse un sistema de videovigilancia sometido a esa única exigencia, se frustraría el legítimo objetivo empresarial de identificar a sus autores, sostiene Garcia-Perrote, pues sobre la empresa, que es también titular del derecho fundamental a la tutela judicial efectiva sin indefensión y a utilizar los medios pertinentes para su defensa (artículo 24.1 y 2 CE), recae la carga de la prueba. Suficiente esa única exigencia para el Tribunal Constitucional, la utilización por los tribunales españoles de pruebas obtenidas mediante grabaciones de cámaras de vigilancia ocultas, con vulneración del derecho de las trabajadoras despedidas a la vida privada del artículo 8 del Convenio Europeo de Derechos Humanos, para declarar la procedencia de su despidos por la comisión de los ilícitos laborales grabados de manera encubierta, no se opuso, sin embargo, al derecho a un proceso equitativo garantizado por el artículo 6.1 de dicho Convenio, ya en el criterio la primera Sentencia del Tribunal Europeo de Derechos Humanos, de 9 de enero de 2018,

en el caso *López Ribalda y otros c. España*. La Sentencia fue revocada por la segunda Sentencia, dictada en el mismo caso por la Gran Sala, el 17 de octubre de 2019, que tampoco apreció vulneración del derecho a la privacidad de las trabajadoras por su grabación encubierta ante las sospechas razonables de robo de la empresa, debidamente ponderadas por los tribunales españoles.

La grabación de sonidos en el lugar de trabajo es excepcional (en la línea de la Sentencia del Tribunal Constitucional 98/2000, de 10 de abril, caso *Casino de La Toja*), sometida su posibilidad a la existencia de riesgos relevantes para la seguridad de las instalaciones, bienes y personas, respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en el artículo 89 de la Ley Orgánica 3/2018.

De particular interés es el análisis de los «sistemas de denuncias internas» en las empresas, de cuya «existencia» deben «ser informados» los «empleados y terceros», al hilo de la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de personas que informen sobre las infracciones del Derecho de la Unión de 23 de abril de 2018, convertida en Directiva *whistleblowing* 2019/1937, de 23 de octubre.

En fin, el profesor García-Perrote no descuida ningún aspecto importante en la miscelánea de cuestiones con que agota el análisis de la Ley Orgánica 3/2018 en su aplicación a las relaciones laborales.

2

LA PROTECCIÓN DE DATOS, EN LA ENCRUCIJADA ENTRE EL DERECHO DE LA UNIÓN Y LA CONSTITUCIÓN ESPAÑOLA

JUAN LUIS REQUEJO PAGÉS
Letrado del Tribunal de Justicia de la Unión Europea

2.1. PREFACIO

La información es poder. En particular, la información sobre los datos personales del individuo puede comportar para quien la detenta una posición de dominio incompatible con los presupuestos de la libertad. Si el constitucionalismo es, en esencia, una técnica de la limitación del poder, la protección de los datos personales constituye una de sus tareas más urgentes en el siglo XXI, cuyas primeras décadas ya perfilan con cierta nitidez el nacimiento de lo que ha dado en llamarse el «capitalismo vigilante».

La naturaleza transnacional del fenómeno de la captación, el tratamiento y la utilización de los datos personales requiere para su control un instrumentario normativo y jurisdiccional que ningún Estado nacional está en condiciones de ofrecer. A la dimensión global del problema sólo cabe oponer una solución no menos universal, hoy por hoy irrealizable. Con todo, el empeño de la Unión Europea en proveer un régimen propio de protección y garantía supone arbitrar una respuesta de alcance continental que, insuficiente todavía frente a un fenómeno global, puede hacerse oír con mayor eficacia que las soluciones ofrecidas por los Estados nacionales.

Un examen siquiera superficial del régimen europeo de protección de datos personales invita a un cierto optimismo en términos de garantías constitucionales. Erigido en objeto de un derecho fundamental por el artículo 8 de la Carta, su tratamiento normativo y jurisprudencial ha dado lugar a un sistema de garantías muy notable. Sin embargo, la articulación de ese sistema con los establecidos por los Estados miembros suscita no pocas dificultades, hasta el punto de llegar a hacer imposible su convivencia y poner en riesgo, en última instancia, la posición del ciudadano.

No se trata solo de dificultades derivadas de la conjunción de sistemas normativos que no comparten una norma constitucional común, esto es, de las dificultades inherentes a la esencia misma del proceso de integración. La dificultad de fondo es una dificultad de principio. La que media entre un ordenamiento ideado para la libertad de mercado y otro nacido para la defensa de la libertad del individuo.

2.2. EL NACIMIENTO DE UN DERECHO FUNDAMENTAL

Con las cuatro décadas que separan a la Constitución Española de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LO 3/2018) no han transcurrido sólo 40 años. En ese tiempo se ha conformado una realidad tan distinta de la que imperaba en 1978 que puede hablarse con propiedad de la sucesión de dos mundos diferentes. A una realidad que entonces no sabíamos que era analógica le ha seguido la del mundo digital, fruto de una revolución que, además de tecnológica, ha sido ante todo conceptual, como sólo pueden serlo los cambios que, afectando a la percepción misma de la realidad, hacen necesaria una verdadera reconstrucción intelectual del mundo[1].

En 1978 no existía Internet. La idea de lo que muchos años más tarde serían Google, Facebook o Twiter habría resultado entonces un propósito inalcanzable. En ese contexto tan sólidamente analógico, la Constitución Española alcanzó a anticipar una tímida garantía frente a una revolución todavía por venir. En su artículo 18, consagrado a la garantía del ámbito de la privacidad, introdujo un apartado 4 en el que se obliga a la ley a limitar «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». Se trataba, en origen, de un mandato al legislador en orden a la mejor protección de dos derechos fundamentales (honor e intimidad) y, con carácter general, al ejercicio pleno de los derechos del ciudadano. Su componente reactivo se cifraba en la legitimación del individuo para recabar la tutela judicial frente a intromisiones en el honor o la intimidad producidas por agresiones ocasionadas por una deficiente li-

1. El construido por la racionalidad occidental se ve seriamente amenazado por la racionalidad puramente inductiva que es consustancial a la gestión masiva de datos. Si aquella se fundamenta en el principio de causalidad, el de esta última lo hace en el de correlación, que permite analizar fenómenos complejos sin conocer y comprender sus causas. En este sentido, Adrien Basdevant y Jean-Pierre Mignard, *L'empire des données*, Don Quichotte, París, 2018, p. 71.

mitación legislativa de la informática. No era identificable, por tanto, en el apartado 4 del artículo 18 de la CE, un derecho constitucional autónomo a la protección de datos, sino una garantía normativa al servicio de los derechos al honor, a la intimidad y a la propia imagen protegidos en el apartado 1 del mismo precepto[2], en una variante que hacía pensar sobre todo en una amenaza para estos derechos procedente del poder público y no tanto de los particulares.

La configuración de un verdadero derecho fundamental autónomo a la protección de datos personales no tardaría, sin embargo, en llegar. Será con ocasión de la STC 292/2000, de 30 de noviembre, cuando el Tribunal Constitucional afirme que «el constituyente quiso garantizar mediante el actual art. 18.4 de la CE no sólo un ámbito de protección específico, sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto[3]». Para el Tribunal, «el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno», en tanto que el derecho a la protección de datos «garantiza a los individuos un poder de disposición sobre esos datos[4]».

Esta última afirmación sólo se entiende en el contexto del desarrollo extraordinario de las técnicas de gestión masiva de datos personales. Un fenómeno que ha alcanzado tales dimensiones que el gigantesco volumen de los datos recabados por las grandes plataformas ha hecho posible que, aun prescindiendo de los datos de carácter estrictamente personal, el resultado de su tratamiento arroje una información muy precisa sobre nuestra identidad y nuestra conducta. Un dato que no es personal en origen puede terminar siéndolo por agregación, comparación o cotejo con bases en las que se contengan otros datos, incluso anonimizados[5].

Los datos de todo orden se han convertido así en un bien extraordinariamente valioso, por cuanto su gestión puede deparar enormes beneficios económicos[6]. Frente a ello no cabe el recurso a la simple patrimonialización de los datos en beneficio de la persona, ya que su valor es en realidad fruto de su tratamiento por un tercero, cuyo presupuesto es la libre circulación de aquellos. De ahí que la fórmula arbitrada por el Tribunal Constitucional de un *derecho al control sobre el flujo de información que concierne a la persona* sea particularmente adecuada, por cuanto concilia el fenómeno de la circulación de los datos –condición de su valor– y el interés del individuo respecto de toda la información que pueda afectarle[7].

La mercantilización de los datos personales es sólo, sin embargo, una parte del problema, y acaso la menor.

---

2. Así, STC 254/1993, de 20 de julio, FJ. 6.
3. STC 292/2000, de 30 de noviembre, FJ. 4.
4. *Loc. ult. cit.I*,, FJ 6.
5. Adrien Basdevant y Jean-Pierre Mignard, *L'empire des données*, cit., p. 116, donde se refiere la posibilidad de que, partiendo de cuatro datos espacio-temporales, se identifique al 90% del total del millón de personas que han realizado operaciones con una tarjeta de crédito en el espacio de tres meses.
6. Los ingresos del mercado mundial de datos habrían alcanzado los 54 millardos de dólares en 2017, previéndose un incremento del 11,2% en los cinco años siguientes; Dan Vesset *et al.*, *Worldwide Big Data and Analytics Software Forecast, 2018-2022*, https://www.idc.com/getdoc.jsp?containerId=US44243318.
7. En este sentido, Vincenzo Cuffaro, «Il diritto europeo sul trattamento dei dati personali», en *Contrato e Impresa* 3/2018, p. 1105.

2.3. UN NUEVO LEVIATÁN

El problema de fondo planteado con el tratamiento de los datos personales es esencialmente el problema de la libertad. No se trata únicamente de que los procedimientos informáticos puedan violentar el ámbito de la privacidad; ni siquiera de que en manos del poder público permitan exponer al ciudadano a un escrutinio incompatible con la dignidad. Es algo más grave.

La gestión de los datos relativos a la conducta de la persona permite la *elaboración de perfiles*, operación definida por el Reglamento (UE) 2016/679[8], como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física[9]». Ello hace posible establecer modelos de comportamiento y, más allá de personalizar la respuesta más adecuada a cada conducta, también anticiparla.

Los famosos algoritmos permiten clasificar a los individuos en función de sus preferencias, elecciones y comportamientos, y convertirlos en objeto de tratamientos diferenciados. Al conjunto de los grupos en los que está integrado el individuo por razones de orden natural (sexo, raza, edad), jurídico (nacionalidad, estado civil, filiación) o por libre decisión de su voluntad (religión, ideología, profesión), se añaden una infinidad de estamentos a los que se le incorpora sin que llegue a tener conciencia de ello y cuya configuración responde a perfiles definidos a partir de una pluralidad de datos en cuyo tratamiento no se atiende a las causas o a la motivación de la conducta, sino al resultado de la correlación entre todos ellos.

La ignorancia acerca de la existencia de los grupos así constituidos supone un problema para la garantía normativa de la igualdad ante la ley, «sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social», según quiere el artículo 14 de la CE. Factores todos ellos protagonistas en la definición de unos perfiles articulados precisamente alrededor de la diferencia. Pero también para la realización material del principio de igualdad, que de acuerdo con el artículo 9.2 de la CE ha de hacerse efectiva respecto del individuo «y de los grupos en que se integra», siendo así que mal podrá intentarse siquiera en aquellos grupos en los que el individuo ha sido «integrado» de manera inopinada.

Ahora bien, la integración en estos últimos grupos no responde a una simple vocación taxonómica. Tras ella viene la respuesta del sistema, tan ciega a la causalidad como la propia recopilación de datos y, en consecuencia, tan automática como implacable. Hasta el punto de que, como pura reacción al comportamiento perfilado por el sistema, puede anticiparse a la materialización misma de una conducta que en realidad es sólo probable. Aparece así el universo siniestro de la policía preventiva. Nada más seguro que excluir del crédito financiero a quien arroja un perfil

8. Reglamento del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
9. Artículo 4, apartado 4), RGPD.

sospechoso, por más que no haya incurrido jamás en un impago; o anticiparse al delito neutralizando al delincuente potencial[10].

El ciudadano se encuentra así integrado, sin saberlo, en grupos que desconoce y sometido a una normatividad que también le es desconocida, aplicada de manera automatizada y sin intervención humana inmediata[11]. Así descritas, las circunstancias de este paisaje se asemejan mucho a las de un momento histórico que teníamos por superado. Aquel en el que el individuo, como el campesino durante la Guerra de los Treinta años, «ignoraba de dónde podría venirle el mal que tantos administraban[12]».

No hay mucha exageración en lo anterior. Garantías elementales del Estado de Derecho como la seguridad jurídica, la publicidad de las normas o la responsabilidad de los poderes públicos son sencillamente inoperantes en un contexto en el que los criterios determinantes de la regularidad de nuestra conducta, esto es, las normas que condicionan y a la postre dirigen nuestro comportamiento[13], vienen dictadas por actores que se desenvuelven en instancias de imposible o muy difícil acceso al poder regulador del Estado. Las garantías constitucionales pueden todavía operar frente a la utilización de las técnicas informáticas por parte de los poderes públicos nacionales, pero pueden muy poco frente a las grandes plataformas digitales, todas ellas localizadas muy lejos de sus fronteras y ya tan poderosas como para cuestionar la voluntad de los Estados.

Se cierne así sobre el individuo un poder de una fuerza formidable, capaz de condicionar su conducta de manera imperceptible y, sobre todo, de definir las circunstancias de su ámbito vital hasta el punto de comprometer la autonomía necesaria para el ejercicio de la libertad. Quien no sabe que la razón de su despido laboral obedece al desafortunado perfil que ha podido componerse con el tratamiento de unos datos cuya existencia desconoce, podrá preguntarse *qué delito ha cometido* con tanta incredulidad y desesperación como Segismundo, y también como él sin poder darse otra respuesta que la de atribuir su desgracia al capricho de la fortuna. Sin embargo, así como en un caso la fortuna no era otra cosa que un padre cruel, mezquino y asustado, en el otro habrá sido un empleador avisado por otro oráculo: el ojo vigilante de las plataformas de gestión de datos, titulares de un poder escrutador tan omnisciente y agresivo que ha sido capaz de dar forma a lo que ya se anuncia como una nueva versión del capitalismo: el capitalismo vigilante[14].

---

10. Adrien Basdevant y Jean-Pierre Mignard, *L'empire des données*, cit., pp. 98-99, dan cuenta de un suceso escalofriante: el de un ciudadano de Wisconsin condenado a seis años de prisión por una sentencia dictada sobre la base de un algoritmo que, de acuerdo con el juez, «le identificaba como un individuo que constituía un alto riesgo para la comunidad». El condenado ni siquiera pudo acceder al algoritmo, ya que estaba protegido por el secreto comercial. La condena sería confirmada en apelación, pero sustituyendo el veredicto informático por el juicio que resultaba del examen de sus antecedentes. Algo no menos perverso, pero sí más humano.
11. Dice mucho del mundo en que vivimos el hecho de que haya sido necesario erigir el «derecho a obtener intervención humana», mencionado en el artículo 22.3 del RGPD y tan anhelado en los episodios de desesperación a los que conduce con tanta frecuencia el «diálogo» con las máquinas. La humanidad ha pasado de hacer cuestión de la intervención divina a contentarse ya sólo con la intervención humana. La razón para esa notable reconsideración de sus expectativas es que, mientras buscaba a Dios mirando al cielo, ha tropezado aquí en la tierra con el diablo del infierno digital.
12. Juan Luis Requejo Pagés, *El sueño constitucional*, KRK, Oviedo, 2016, p. 41.
13. Una norma no es otra cosa, al cabo, que un criterio vinculante de regularidad, en la definición aquilatada de Alessandro Passerin d'Entrèves, *La noción del Estado*, traducción de Antonio Fernández Galiano, Ariel, Barcelona, 2001, p. 102.
14. Shoshana Zuboff, *The Age of Surveillance Capitalism*, Profile Books, Londres, 2019.

De la gestión y el tratamiento de los datos personales se ha pasado, imperceptiblemente, al tratamiento de la personalidad mediante la inducción de conductas. Del gobierno por la voluntad del pueblo, a la voluntad popular gobernada por los gestores de los datos de las personas que lo componen.

Allí donde, como es el caso, aparece un problema para la libertad se hace perentorio el auxilio del constitucionalismo. Como técnica ideológica al servicio de la limitación del poder en beneficio de la libertad, el constitucionalismo tiene en la sujeción de los actores del universo digital su empresa más urgente en los próximos decenios. Enfrente no tiene ahora, como en los siglos XVIII y XIX, a los monarcas absolutos, ni a los partidos totalitarios del siglo XX, sino a los *poderes digitales*, un agregado de plataformas de tratamiento y gestión de datos, de sociedades mercantiles y de poderes públicos que han constituido una criatura capaz de rivalizar con Leviatán y disputarle el poder soberano sobre la vida y la libertad del ciudadano.

2.4. LA ESPERANZA EUROPEA

Las dimensiones del fenómeno digital requieren una intervención de corte constitucionalista que no está en la mano de los Estados nacionales. Su tratamiento exigiría un ordenamiento jurídico tan universal y efectivo como los poderes digitales de cuya contención se trata. En ausencia de un Estado global queda el remedo de las soluciones regionales, como la que puede dispensar la Unión Europea en tanto que autoridad continental. Una solución limitada y de alcance, cuyo principal inconveniente es que a día de hoy ninguna de las grandes sociedades gestoras de datos personales tiene su sede en el territorio europeo. Pero en todo caso más efectiva que la que puede esperarse de los Estados nacionales.

El aparato normativo y jurisprudencial con el que se ha dotado la Unión Europea para este lance responde, en apariencia al menos, al modelo clásico de los instrumentos de garantía ideados por el Estado constitucional.

El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la Carta) consagra el derecho a la protección de los datos personales. Sobre la base de una jurisprudencia de marcado aliento garantista[15], el legislador europeo ha culminado un laborioso proceso normativo con la aprobación del RGPD, que pone en planta una disciplina del tratamiento de datos verdaderamente ambiciosa y notable[16].

---

15. Son referencia inexcusable las sentencias de 8 de abril de 2014, *Digital Rights Ireland y otros* (C-293/12 y C-594/12, EU:C:2014:238), de 13 de mayo de 2014, *Google Spain y Google* (C-131/12, EU:C:2014:317), de 6 de octubre de 2015, *Schrems* (C-362/14, EU:C:2015:650) de 19 de octubre de 2016, *Breyer* (C-582/14, EU:C:2016:779), o de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros* (C-203/15 y C-698/15, EU:C:2016:970), así como el Dictamen de 26 de julio de 2017 [A-1/15 (*Acuerdo PNR UE-Canadá*), EU:C:2017:592].
16. Los hitos normativos más relevantes en ese proceso han sido la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y el Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos; y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el

La ambición del RGPD se demuestra ya en la definición del ámbito territorial de su vigencia, que no se circunscribe al territorio de la Unión. Sus normas han de aplicarse, con arreglo a su artículo 3, apartado 2, a todo «tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con a) la oferta de bienes o servicios [...] o, b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión». Vocación de extraterritorialidad que se antoja inexcusable en el tratamiento de un fenómeno global y que se concreta en la obligación de que los responsables o encargados del tratamiento de datos no establecidos en la Unión designen un representante en uno de los Estados miembros cuando sea de aplicación el citado artículo 3, apartado 2[17].

La relación de los principios que inspiran al RGPD se cifran en la licitud, la lealtad, la transparencia y el consentimiento[18], sustanciándose en derechos tales como el derecho a la información y al acceso[19], a la rectificación, supresión («derecho al olvido») y limitación[20], a la portabilidad de los datos[21] o el ya mencionado a la intervención humana[22]. Un extenso capítulo dedicado al responsable y al encargado del tratamiento de datos, a la seguridad de estos últimos, a la evaluación de impacto relativa a su protección, al delegado de protección de datos y a los códigos de conducta y certificación[23], va seguido de una pormenorizada disciplina de la transferencia de datos personales a terceros países u organizaciones internacionales[24], que se completa con sendos capítulos dedicados a las autoridades de control[25] y al régimen de recursos, responsabilidad y sanciones[26].

El conjunto no puede ser más pormenorizado, y en una primera impresión no cabe negarle un espíritu garantista que le confiere un inequívoco aire de familia con los instrumentos de protección de derechos típicamente constitucionales.

No obstante, y sin necesidad de entrar aquí en un examen de detalle que no viene ahora al caso, esa impresión se desvanece a poco que nos aproximemos al RGPD desde la perspectiva de los principios y de los conceptos. Así examinado, el RGPD ofrece una imagen muy distinta, hasta el punto de aparecer antes como un problema constitucional que como un instrumento al servicio del constitucionalismo.

En realidad, no cabía esperar otra cosa.

---

sector de las comunicaciones electrónicas.

17. Artículo 27, apartado 1. Obligación que no será aplicable, con determinadas reservas, al tratamiento ocasional y en ningún caso a las autoridades u organismos públicos (apartado 2).
18. Artículos 5 a 11.
19. Artículos 13 a 15.
20. Artículos 16 a 19.
21. Artículo 20.
22. Artículo 22.
23. Capítulo IV, artículos 24 a 43.
24. Capítulo V, artículos 44 a 50.
25. Capítulos VI y VII, artículos 51 a 59 y 60 a 76.
26. Capítulo VIII, artículos 77 a 84, al que sigue un capítulo dedicado a situaciones específicas de tratamiento en relación con las libertades de expresión y de información (artículo 85), el acceso a documentos oficiales (artículo 86), el número nacional de identificación (artículo 87), el ámbito laboral (artículo 88), las finalidades de archivo, de investigación científica, histórica o estadística (artículo 89), las obligaciones de secreto (artículo 90) o las iglesias y asociaciones religiosas (artículo 91).

2.5. LA UNIÓN COMO AMENAZA

El RGPD es fiel al espíritu del Ordenamiento en el que ha nacido y al que en última instancia se debe. No hay en él traición alguna a los principios del constitucionalismo, sencillamente porque esos principios no son los constituyentes del Derecho de la Unión, sino sólo una parte de los que le inspiran en la ejecución de los principios que le son resueltamente propios y que lo definen y fundamentan como un orden normativo autónomo: los principios del mercado.

La Unión ha sido, hasta tiempos muy recientes, una serie de Comunidades constituidas al servicio de un mercado. Pese a que desde un principio dieron muestras de una ambición que acreditaba una cierta vocación paraestatal, sólo en 1992 abandonaron formalmente su condición comunitaria para adoptar la identidad de una Unión de Estados, haciéndose entonces evidente que el *principio de primacía* sobre el que se había venido constituyendo la autonomía del Derecho Comunitario comportaba en su lógica interna una irreprimible voluntad soberana[27]. La aprobación del Tratado de Lisboa y, en particular, la entrada en vigor de la Carta, ha sancionado de manera muy poco disimulada las pretensiones estatalistas de la Unión.

No es cuestión de entrar aquí en los pormenores del proceso que ha venido haciendo de la integración europea, casi desde el principio, un verdadero proceso constituyente, en el que todavía estaremos por mucho tiempo y del que no podemos aventurar si terminará con la constitución de un Estado continental o con el regreso a la plena soberanía de los viejos Estados nacionales[28]. Pero sí ha de insistirse en que la aprobación de la Carta, lejos de abundar en la consolidación del régimen de derechos individuales garantizados por las Constituciones de los Estados miembros, puede ponerlos en grave peligro. El caso de la protección de los datos de carácter personal constituye, justamente, el mejor de los ejemplos.

La Unión, que (todavía) no es un Estado, cuenta con una Carta de derechos. Lo primero supone que sus competencias no son ni originarias ni completas, sino atribuidas y sectoriales, con la consecuencia de que su Derecho no puede regir todos los ámbitos en los que se desenvuelve la actividad del individuo. Lo segundo, la Carta, comporta una declaración de derechos equivalente a las recogidas en las Constituciones nacionales, cuya vocación natural es la de disciplinar en su totalidad las relaciones del individuo con el poder público. Se ha instalado así en el seno de la Unión Europea una institución que tiene su sede natural en los Estados, pero no (todavía) en aquella.

En efecto, la ambición normativa de las Cartas constitucionales se corresponde con la omnipotencia reguladora de los poderes públicos nacionales, establecidos por obra de una Constitución que erige y distribuye ámbitos competenciales absolutos. En cambio, la ambición de la Carta no encuentra simetría en las competencias

27. La convivencia entre el Derecho Comunitario o de la Unión y los Derechos de los Estados miembros se ha garantizado tradicionalmente sobre la base de un silencio interesado acerca de la radical incompatibilidad de fondo entre los dos principios (primacía y soberanía) que fundamentan la existencia de ambos órdenes normativos. Al respecto, Juan Luis Requejo Pagés, «Primacía de la Unión y soberanía nacional», en *Libro homenaje a Pedro Cruz Villalón* (en prensa).
28. Que ese sería el final deseable para esta larga historia me parece una conclusión tan razonable como imposible. Juan Luis Requejo Pagés, *El sueño constitucional*, cit.

derivadas y tasadas de la Unión. Y esta asimetría produce unos efectos extraordinariamente perturbadores.

La vocación naturalmente expansiva de los derechos[29], justamente por definitorios del estatuto de la persona en el contexto de un sistema que, por democrático, tiene en ella el fundamento de su legitimación política, se compadece difícilmente con sistemas normativos que no pueden regir todos los ámbitos de actividad del ciudadano.

Pese a todas las cautelas intentadas con el artículo 51 de la propia Carta y con el artículo 6, apartado 1, del Tratado de la Unión (TUE), la Carta ha supuesto que la Unión haya quedado sometida a dos principios contradictorios, si no excluyentes. Sigue siendo, ante todo, una comunidad económica al servicio de unos fines para los que cuenta con un dominio de competencias tasadas. Pero es también un sistema de normas comprometido con la defensa de los derechos y no sólo con la garantía de las cuatro libertades. A la limitación de competencias que implica lo primero se superpone un deber de protección sólo realizable por un poder plenamente competente.

Si la delimitación del ámbito competencial de la Unión se ha enfrentado, desde el principio, a las dificultades planteadas por la vocación expansiva que ha caracterizado desde siempre a las autoridades comunitarias, esa dificultad se hace casi inmanejable desde el momento en que las competencias de la Unión comprenden también el ámbito de los derechos fundamentales. Una circunstancia que se demostrará preciosa para un Tribunal cuyo activismo en el proceso de integración ha sido fundamental para que el Mercado Común se haya convertido en la Unión que hoy conocemos. Con muchos menos mimbres que los que le ofrece el Tratado de Lisboa, el Tribunal de Justicia ha sido capaz de construir los principios de primacía y de eficacia directa. Disponiendo ahora de la Carta –con toda la potencialidad expansiva que, en términos competenciales, es inherente a una declaración de derechos–, el Tribunal de Justicia no puede sino interpretar de manera restrictiva las disposiciones de la Carta que condicionan y limitan su propia interpretación y aplicación[30].

El efecto expansivo de la Carta supone un problema de enorme envergadura desde el punto de vista de la definición de los ámbitos competenciales respectivos de la Unión y de los Estados miembros. Pero todavía más notable es el problema que comporta la inevitable atribución al Tribunal de Justicia de la competencia para interpretar los derechos fundamentales de la Unión. En nuestro caso, la consideración de la Carta como uno de los tratados a los que el artículo 10.2 de la CE atribuye la condición de norma vinculante para la definición de los derechos fundamentales reconocidos por la Constitución confiere a la jurisprudencia del Tribunal de Justicia un valor definitorio al que no puede sustraerse el Tribunal Constitucional[31].

---

29. Es paradigmático el supuesto del derecho a la tutela judicial efectiva, cuyo reconocimiento implica la judicialización de todo el ordenamiento y, con ella, la necesidad de que este se estructure a través de procedimientos que, por su sola existencia, no pueden dejar de condicionar el contenido material de las disposiciones que de ellos resultan. En términos más generales, la lógica de la expansividad de los derechos fundamentales y su objetivación como valores del ordenamiento más allá de su dimensión subjetiva originaria forma parte del patrimonio compartido de los ordenamientos constitucionales que, con más o menos consecuencia, han hecho suya la doctrina *Lüth* del Tribunal Constitucional alemán.
30. Sobre el particular, Juan Luis Requejo Pagés, «El futuro de un vértice jurisdiccional cada vez más complejo», en *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid* 22 (2018), pp. 122 y ss.
31. Con carácter general Juan Luis Requejo Pagés, «El futuro de un vértice jurisdiccional cada vez

El problema que comporta la pluralidad de enunciados de un mismo derecho fundamental puede resolverse si se logra reducirlos a unidad mediante una interpretación que, con independencia de cuál haya de ser la instancia jurisdiccional legitimada para llevarla a cabo, permita la definición material de un único derecho armónico y coherente. Pero cuando, como es el caso, los intérpretes jurisdiccionales en liza son custodios de órdenes normativos que sólo tangencialmente responden al mismo espíritu, el riesgo de que el sistema de los derechos fundamentales se vea sometido a tensiones que lo derrumben puede darse por descontado.

Lamentablemente, este es el contexto en el que hay que abordar la lectura del RGPD.

2.6. LOS DERECHOS EN SU CONTEXTO

El artículo 1 del RGPD no llama, desde luego, a engaño cuando en su apartado 3 declara que "[l]a libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". Como su propio nombre indica[32], el RGPD no tiene por único objeto la protección de los datos personales, sino también la garantía de su libre circulación. Si aquella constituye un

más complejo», cit. *passim*. A este respecto, la doctrina establecida por el Tribunal de Justicia en el asunto *Melloni* (sentencia de 26 de febrero de 2013, C-399/11, EU:C:2013:107) ilustra bien el problema de principio al que se enfrenta el Tribunal Constitucional como intérprete cualificado (que no exclusivo, dada la autoridad *constitucional* del Tribunal Europeo de Derechos Humanos) de los derechos fundamentales vigentes en España.

32. Reglamento «relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos».

derecho fundamental, esta es una manifestación del ejercicio de las cuatro *libertades fundamentales* para cuya defensa se han erigido primero las Comunidades y después la Unión.

De ahí la preocupación del legislador de la Unión por cohonestar aquel derecho y esta libertad. Operación en la que es de advertir un sesgo relativamente sutil en beneficio de esta última. Así, en el considerando (4) del RGPD se afirma que el primero «no es un derecho absoluto[,] sino que debe considerarse en relación con su función en la sociedad y mantener un equilibrio con otros derechos fundamentales», mencionándose, en particular, la libertad de empresa. En esa línea, y tras destacar en el considerando (5) que «[l]a integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales», señalando que «[e]n toda la Unión se ha incrementado el intercambio de datos personales entre operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas», afirma el legislador que «[e]l Derecho de la Unión insta a las autoridades nacionales [...] a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro».

Es innegable que la protección de los datos personales constituye el objeto del RGPD. Pero no es su objeto exclusivo, pues con el mismo título se acomoda en su estructura la garantía de su libre circulación. Y si está en el propósito del legislador proveer a la mejor protección de los datos de carácter personal, también lo está que esa protección se dispense de manera uniforme y no fragmentada, pues, como se afirma en el considerando (9), «[l]as diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, [...] pueden impedir la libre circulación de los datos de carácter personal en la Unión», constituyendo «un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, [falseando] la competencia e [impidiendo] que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión».

A estas reveladoras declaraciones del legislador cabe añadir todavía la del considerando (10), en el que se afirma que si el nivel de protección de los derechos y libertades en relación con el tratamiento de los datos personales debe ser equivalente en todos los Estados miembros, ello es con el fin de «garantizar un nivel uniforme y elevado de protección de las personas físicas», pero también para «eliminar los obstáculos a la circulación de datos personales dentro de la Unión».

Todo parece indicar, en definitiva, que lo que verdaderamente importa no es sólo, ni tanto, la protección de los datos personales, cuanto también el buen funcionamiento del mercado. Este sería, en realidad, el objetivo primero del RGPD, lo que resulta perfectamente coherente con el espíritu propio de la Unión, bajo cuya apariencia resueltamente paraestatal sigue latiendo el corazón del mercado.

A este respecto no puede olvidarse que el universo de los derechos fundamentales sólo se ha incorporado a la estrategia del proceso de integración en la medida en que los Estados miembros (vale decir, el Tribunal Constitucional alemán) han hecho de su respeto una condición de la construcción europea. No se trata, por tanto, de un universo propio, sino de un mundo radicalmente extraño y que las instituciones de la Unión vienen obligadas fatalmente a conllevar. De ahí que, adelantando la descarnada proposición del artículo 1, apartado 3, del RGPD, en el considerando (13) se lea que «[e]l buen funcionamiento del mercado interior [esto sería lo que en verdad importa] exige que la libre circulación de los datos personales no sea restringida ni prohibida

por motivos relacionados con la protección [...] de datos personales» [unos motivos –esto parece– a los que no puede dejar de atenderse *en la medida* en que constituyen el tributo que debe pagarse para que no se detenga el proceso de integración].

2.7. LA ILUSIÓN DE LA CONCORDIA

Las palabras, las categorías y los conceptos del RGPD podrían constituir un instrumento normativo de muy notable calidad jurídica en el seno de un Ordenamiento nacional como el de cualquiera de los Estados miembros. En ese contexto, los desequilibrios en favor de la libertad de circulación podrían corregirse mediante una interpretación integradora basada en el espíritu de sistema del orden constitucional, cuyo fundamento primero no se encuentra en el mercado ni en las libertades económicas, sino en la dignidad de la persona y en la limitación del poder público al servicio de la libertad individual. En un contexto, en definitiva, en el que la persona no es un mero consumidor, sino un auténtico ciudadano.

Sin embargo, tanto en el ámbito de los derechos fundamentales, en particular, como en el de la articulación entre el Derecho de la Unión y los Derechos nacionales, en general, sigue operando la *ilusión de la concordia* que está en la base de la solución de compromiso que ha hecho posible llegar tan lejos en el proceso de la integración europea.

El lenguaje jurídico-formal de las Constituciones y de los Tratados se refiere, con plena conciencia de la impostura, a una realidad que se sabe desmentida por la lógica del principio de primacía. Si las formas procuran a los Estados miembros cierta tranquilidad en cuanto a su condición (formal) soberana, la prevalencia permite a la Unión comportarse en la práctica como un auténtico soberano (material). De la indiferenciación interesada entre lo formal y lo material nace el equívoco sobre el que se articulan las relaciones entre la Unión y los Estados. Un equívoco que permite a estos la ilusión de la soberanía y a aquella la eficacia de un poder incontestable (y, por ello, a la postre, soberano)[33].

La comunión de las palabras evoca así una armonía bajo la que se oculta una discordia conceptual insuperable. Tal es también el caso con los derechos reconocidos a la par por las Constituciones y por la Carta. La lengua de los derechos no sirve tanto para entenderse como para engañarse. Creyendo hablar de lo mismo cuando la Constitución Española garantiza el derecho a la tutela judicial efectiva en su artículo 24 que cuando lo hace la Carta en su artículo 47, el Tribunal de Justicia nos ha enseñado en el asunto *Melloni*[34] toda la realidad que separa a las palabras de ambos preceptos.

Con todo, en el supuesto de la protección de datos, las palabras mismas de los legisladores revelan ya, si no alguna desarmonía, sí una cierta discrepancia en sus respectivos intereses.

Así, mientras el legislador de la Unión ha titulado su RGPD refiriéndolo «a la *protección* de las personas físicas en lo que respecta al tratamiento *de datos personales* y a la *libre circulación* de estos datos», el legislador orgánico ha adaptado el Derecho español a aquel Reglamento con una Ley Orgánica «de *protección de datos personales* y *garantía de los derechos digitales*». Sin asomo, por tanto, de la libre circulación de datos

33. Juan Luis Requejo Pagés, «Primacía de la Unión y soberanía nacional», cit.
34. *Melloni* (C-399/11, EU:C:2013:107).

y con énfasis redoblado en la vertiente protectora del derecho individual, ampliada a los denominados «derechos digitales».

Ambos textos normativos son expresión de dos sensibilidades muy distintas. Si, como antes se ha visto, el legislador de la Unión lamenta en el considerando (9) del RGPD que la Directiva 95/46 no haya podido evitar una fragmentación en los niveles de protección que puede «impedir la libre circulación de datos de carácter personal en la Unión», el legislador orgánico se duele de que el fracaso de la finalidad armonizadora de aquella Directiva haya «conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos[35]».

En definitiva, sin mayor exageración puede concluirse que, en lo que hace al núcleo de las preocupaciones respectivas de ambos legisladores, de un lado tenemos una libertad económica meramente condicionada por un derecho, y de otro un derecho desprovisto de toda consideración instrumental.

2.8. EL CONCIERTO JUDICIAL

Cabe preguntarse entonces si ambos textos normativos, el RGPD y la LO 3/2018, consienten una integración de la que resulte una disciplina coherente y armoniosa del derecho a la protección de datos.

El legislador orgánico no parece haberlo dudado. También a mí me parece que esa operación es posible. El problema es que el precio de esa integración puede ser la desnaturalización del derecho garantizado por el artículo 18.4 de la CE. En otras palabras, que el resultado sea armónico y coherente, pero sólo después de hacer pasar a este precepto constitucional por el lecho de Procusto.

La interiorización del RGPD en el Derecho interno no ha podido ser más radical, desde el momento en que el artículo 1, letra a), de la LO 3/2018 ha hecho de él la norma que, junto con la propia Ley Orgánica, debe regular el ejercicio del derecho a la protección de datos personales, cumpliendo así con la obligación establecida en el artículo 53.1 de la CE[36]. A esa condición privilegiada atribuida al RGPD se suma la que corresponde al artículo 8 de la Carta en virtud del artículo 10.2 de la CE y que hace de la versión europea del derecho fundamental a la protección de datos un elemento definitorio de su concepto constitucional *ex* artículo 18.4 de la CE. Versión cuyo contenido, alcance y eventual evolución están en la mano del Tribunal de Justicia de la Unión Europea.

La definición del derecho constitucional a la protección de datos ha perdido de este modo la perfecta autonomía nacional que le caracterizaba en el momento de la entrada en vigor de la Constitución. O, más precisamente, desde el momento en que, como hemos visto, el Tribunal Constitucional erigió un derecho fundamental propio a partir de la garantía normativa establecida en el artículo 18.4 de la CE. La única intervención exógena en el proceso de definición de ese derecho venía reservada hasta entonces, en virtud del artículo 10.2 de la CE, al Convenio de Roma (CEDH) y sus garantías sobre los derechos de la privacidad. Por sus propias características,

35. Preámbulo de la LO 3/2018, apartado III, párrafo primero.
36. La acción normativa conjunta del RGPD y de la LO 3/2018 cumple así con la reserva de ley en cuanto a la regulación del ejercicio del derecho (artículo 53.1 CE) y con la reserva de ley orgánica por lo que se refiere a su desarrollo (artículo 81.1 CE).

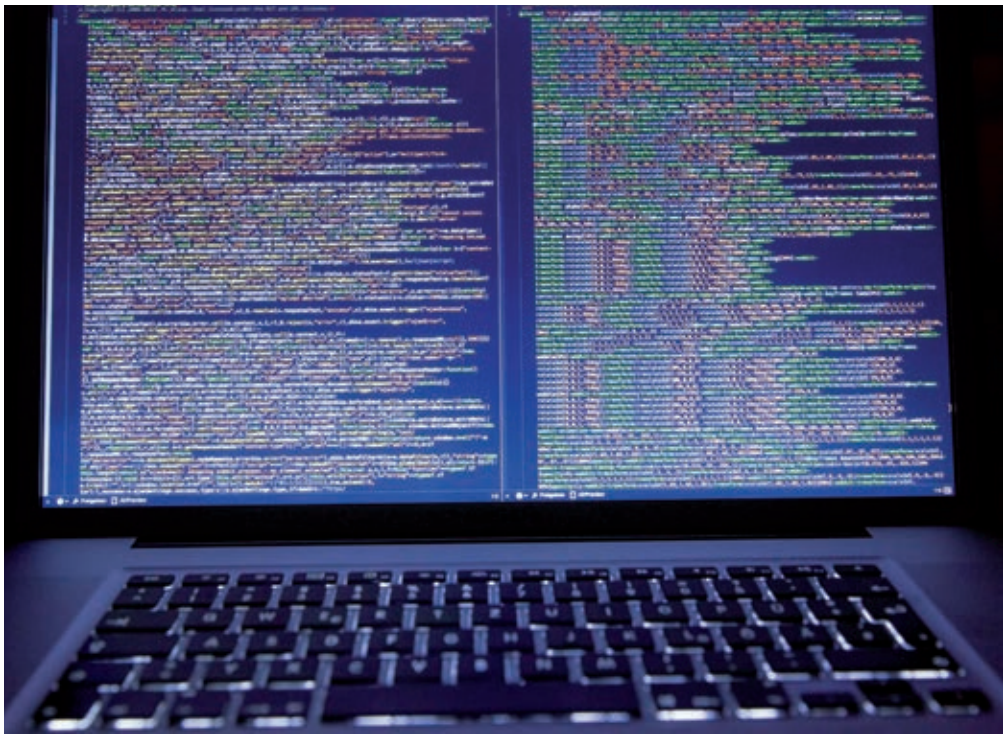
que hacen del Derecho y de la jurisdicción del CEDH un sistema de garantías mínimas[37], la libertad de configuración conceptual de los derechos fundamentales de la que disfrutaba el Tribunal Constitucional era entonces muy considerable. Con la irrupción de la Carta, y en particular de su artículo 8, ha entrado en juego una variante europea del derecho fundamental a la protección de datos que, además de no traducirse en una mera garantía *de minimis*, cuenta para su imposición con todo el aparato y la autoridad del principio de primacía.

El Tribunal Constitucional no puede ya limitarse a incorporar en la definición constitucional del derecho a la protección de datos el contenido mínimo que resulta del CEDH y de su Tribunal, sino que debe definirlo a partir de una versión europea del derecho a la protección de datos que ya es de suyo perfecta y acabada. No se trata ahora de definir el derecho constitucional teniendo en cuenta el contenido mínimo exigido por el CEDH, sino de hacer sitio en el enunciado constitucional a la definición realizada en el Derecho de la Unión por obra de la Carta, del Derecho derivado y del Tribunal de Justicia; una operación que apenas dejará sitio para que aquel enunciado albergue un contenido constitucional genuinamente propio. El Tribunal Constitucional no es ya el señor del derecho fundamental, sino el auxiliar que se cuida de que ese derecho sea en el Derecho interno tal cual se ha definido su homónimo en el Derecho de la Unión.

Ciertamente, aprovechando los muchos espacios abiertos por el RGPD a las autoridades nacionales[38], el legislador orgánico ha emprendido una labor de depuración del orden interno y de acomodación del RGPD que ha deparado una configuración última del derecho a la protección de datos con perfiles característicamente nacionales. Para ello ha tomado pie en el considerando (8) del RGPD, en el que se declara que, allí donde el RGPD «establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos de su propio Reglamento». Quizás la LO 3/2018 ha ido demasiado lejos al interpretar estas palabras en el sentido de que le autorizan a *desarrollar* y *complementar* el Derecho de la Unión[39]. De manera más cautelosa, la Comisión recuerda que la prohibición de repetir el texto de los Reglamentos en el Derecho nacional sólo puede excepcionarse cuando sea estrictamente necesario por razones de coherencia o de inteligibilidad, sin que le quepa al legislador nacional, en relación con el RGPD, «ni interpretarlo [ni] añadir condiciones adicionales a las normas directamente aplicables en virtud del Reglamento[40]».

En cualquier caso, amparado en el RGPD, el legislador orgánico ha decidido, por ejemplo, matizar la inaplicabilidad absoluta decidida por aquel en relación con las personas fallecidas[41] y permitir que las personas vinculadas al fallecido puedan

37. Al respecto, Juan Luis Requejo Pagés, «El futuro de un vértice jurisdiccional cada vez más complejo», cit.
38. Son un total de 57 los reenvíos que en él se hacen a los legisladores, tribunales y autoridades competentes de los Estados miembros.
39. Así da a entenderlo en el apartado III, párrafo cuarto, *in fine*, del Preámbulo.
40. Comunicación de 24 de enero de 2018 de la Comisión al Parlamento Europeo y al Consejo. Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018 [COM(2018) 43 final].
41. Considerandos (27), (158) y (160) del RGPD.



solicitar el acceso a sus datos, así como su rectificación o supresión[42]. Asimismo, el Título X de la LO 3/2018 se ha consagrado al reconocimiento y garantía de una serie de derechos digitales en el ámbito de Internet, concretando en ese terreno las previsiones generales y de principio ya dispuestas en el RGPD.

El resultado ha sido un cuerpo normativo en el que el derecho constitucional a la protección de datos ha sido desarrollado (artículo 81.1 de la CE) y regulado en su ejercicio (artículo 53.1 CE) por un Reglamento europeo de aplicación directa, completado por una Ley Orgánica en los términos en los que el propio Reglamento lo ha permitido. La cuestión sería si el derecho a la protección de datos que así se ha configurado es el que cabía esperar a partir del artículo 18.4 de la CE o más bien el que era inevitable con el artículo 8 de la Carta.

En realidad, la cuestión tiene muy poco sentido. Sólo lo tiene para poner de manifiesto que el derecho del artículo 18.4 de la CE, considerado en sí mismo, apenas tiene que ver con el artículo 8 de la Carta. Aquel es un derecho fundamental reconocido por un Estado erigido a partir de una Constitución que asegura al individuo un estatuto de ciudadanía. Este, en cambio, un derecho reconocido a los consumidores en el ámbito de la libertad de mercado. El problema viene dado por el hecho de que la Unión haya configurado este último derecho como un derecho fundamental. Más aún, por el hecho mismo de haber proclamado una Carta de derechos fundamentales.

Al hacerlo, ha sido inevitable que se desencadenara la lógica del artículo 10.2 de la CE y que el derecho constitucional a la protección de datos se reconfigurara con arreglo al artículo 8 de la Carta, cuyo desarrollo por las instituciones de la Unión se ha visto además favorecido en su eficacia por el principio de primacía.

42. Artículo 3 y 96 del RGPD.

Obedeciendo a espíritus tan dispares –el de la ciudadanía y el del mercado–, la coherencia conceptual es sencillamente imposible, no cabiendo más solución que la de reducir a unidad la contradicción entre ambos modelos mediante la subordinación y el sacrificio de uno de ellos. El principio de primacía del Derecho de la Unión no deja lugar a dudas acerca de cuál ha de ser el sacrificado.

Naturalmente, nada de esto es privativo del derecho a la protección de datos, sino que vale para todos y cada uno de los derechos fundamentales reconocidos por la Constitución Española. Pero en el caso de aquel derecho, la cuestión es particularmente delicada, tanto por la importancia creciente del tratamiento de los datos personales y del riesgo que comporta para la intimidad y la libertad del ciudadano, como por la concreta configuración que ha hecho del mismo el legislador de la Unión en el RGDP, que es por igual, como hemos visto, un instrumento de garantía de los datos y un incentivo para su libre circulación.

En el plano puramente normativo es difícil advertir las diferencias que separan al artículo 18.4 de la CE del artículo 8 de la Carta. Se han hecho más notables en el nivel de la legislación, cuando el RGPD ha equiparado la relevancia de la protección de datos con la libertad de mercado, aunque de manera sólo aparente, pues a la postre es esta la que prevalece. Pero será en el momento de la aplicación cuando se consume, irremediablemente, el triunfo del artículo 8 de la Carta y el de la filosofía que comporta.

Será cuando las autoridades administrativas y, en última instancia, los jueces hayan de ponderar el derecho a la protección de datos con la libre circulación de los mismos cuando fatalmente se imponga a la lógica del derecho del ciudadano la de la libertad del consumidor. En su doble condición de autoridad administrativa nacional y comunitaria, por un lado, y de juez español y de la Unión, por otro, las Administraciones españolas y los Tribunales nacionales no podrán dejar de plegarse al imperativo de la primacía y someterse a la palabra del Tribunal de Justicia. Las esperanzas que puedan cifrarse en el Tribunal Constitucional se demostrarán en último término vanas, pues la cuestión prejudicial del artículo 267 TFUE le ha desprovisto de su condición de juez exclusivo de la ley, ahora difuminada en un Poder Judicial legitimado para cuestionar la legalidad contrastándola con la Carta y ante la autoridad del Tribunal de Justicia[43]. El recurso de amparo le permitirá cumplir con su función de intérprete supremo de la Constitución y, con ese título, abundar en la definición de los derechos fundamentales del Título I. Pero si ha de ser consecuente con el mandato del artículo 10.2 de la CE no puede obviar en ese cometido la jurisprudencia del Tribunal de Justicia en relación con la Carta, sin que pueda valerse siempre de soluciones evasivas y de compromiso como las que le permitieron salir (sólo) aparentemente airoso del trance en el que se vio con ocasión del asunto *Melloni*[44].

El duelo entre el Derecho Constitucional y el Derecho de la Unión es, al cabo, el que se libra entre los Tribunales Constitucionales y el Tribunal de Justicia en una encrucijada en la que se decide la suerte de los derechos fundamentales, particularmente la del derecho a la protección de los datos de las personas. Un duelo en el que

43. Sobre la articulación procesal entre las cuestiones de inconstitucionalidad y prejudicial, Pedro Cruz Villalón y Juan Luis Requejo Pagés, «La relación entre la cuestión prejudicial y la cuestión de inconstitucionalidad», *Revista de Derecho Comunitario Europeo* 50 (2015), pp. 173-194, y Juan Luis Requejo Pagés, «Algunas consideraciones sobre la relevancia constitucional del Derecho de la Unión», en *El Juez del Derecho Administrativo. Libro homenaje a Javier Delgado Barrio*, Marcial Pons, Madrid, 2015, pp. 493-502.
44. *Melloni* (C-399/11, EU:C:2013:107).

no rige el principio de la igualdad de armas, pues si ambos contendientes empuñan sendas espadas, una está forjada con el rígido acero de los derechos y la otra con el más flexible y maleable de las libertades mercantiles. Y quien esgrime esta segunda cuenta, además, con la ventaja que supone atacar y defenderse desde una posición de primacía.

La relación entre el Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos (TEDH) no puede explicarse en términos de duelo o de reyerta. De un lado, porque uno y otro operan en niveles separados dentro del proceso de definición de los derechos, correspondiendo al TEDH la tarea de garantizar un mínimo sobre el que ha de erigirse después el máximo acordado por el Tribunal Constitucional[45]. De otro, porque ambos Tribunales son «tribunales de derechos», familiarizados con las categorías, los principios y las técnicas de la teoría de los derechos fundamentales. Su concurrencia es, por tanto, más colaborativa que beligerante.

En cambio, el Tribunal de Justicia no ha sido nunca un «tribunal de derechos», como tampoco la Unión ha sido una comunidad de derechos hasta que se ha visto forzada a tratar de serlo para sortear los recelos del Tribunal Constitucional alemán. No hay poco, por tanto, de conversión forzada. Y si la Carta no deja de ser un cuerpo extraño en la estructura de una Unión nacida para el mercado, no lo es menos para un Tribunal cuyo universo ha sido siempre el de la libertad de comercio. Ello supone que la palabra decisiva a la hora de configurar los derechos fundamentales del ciudadano europeo se confía a un Ordenamiento en el que, por su origen derivado y su naturaleza sectorial, tienen más sentido y mejor cabida los derechos del consumidor que los del ciudadano, y a un Tribunal poco familiarizado con el espíritu y con la técnica de los derechos fundamentales.

Si la apuesta por la promulgación de la Carta ha de servir para propiciar que el proceso de integración acabe por transmutarse en un verdadero proceso constituyente y culmine con la constitución de la República de Europa, habrá merecido, en mi opinión, la pena. Si, por el contrario, la integración no ha de progresar en esa dirección y se mantiene en las lindes de una comunidad de mercado, será difícil evitar que la lógica mercantil pervierta en mayor o menor grado la naturaleza constitucional de los derechos fundamentales.

Los constitucionalistas se encuentran así ante un dilema diabólico: O hacer de la Unión un Estado y consagrarse a la tarea de que la Carta lo sea de unos derechos fundamentales en el sentido cabal del término para que –así concebida y defendida por un Tribunal de Justicia plenamente consecuente con su condición de tribunal de derechos– inocule en la estructura de la Unión la necesidad de constituirse como un Estado. O esforzarse en reducir la Carta a la condición de un estatuto de los consumidores y marcarle los límites que no puede franquear en detrimento de las cartas constitucionales, apostando definitivamente por el mantenimiento del Estado nacional.

A día de hoy, no faltan razones para confiar en que el Tribunal de Justicia contribuya a escorar la balanza en favor de la primera alternativa. Precisamente es en el ámbito de la protección de datos donde su doctrina permite abrigar alguna esperanza en ese sentido. Con su resuelta determinación de primar la protección de los datos personales frente a la libre circulación de los mismos, sentencias como la

45. Me remito de nuevo a Juan Luis Requejo Pagés, «El futuro de un vértice jurisdiccional cada vez más complejo», cit.

dictada en el asunto *Google Spain*[46] parecen indicar que el Tribunal de Justicia no participa ya del espíritu del mercado con el mismo entusiasmo que todavía demuestra el legislador del RGPD.

Puede tratarse de una impresión equivocada o, quizás, sólo justificada en este concreto sector del Derecho de la Unión, pues la sensibilidad constitucional del Tribunal de Justicia parece todavía un tanto menesterosa en terrenos como el de las garantías penales. Ahí está el asunto *Melloni*[47]. También, muy en particular, el caso *Taricco*[48], si bien en este supuesto el Tribunal de Justicia ha dado prueba de su capacidad de rectificación cuando los Tribunales Constitucionales hacen valer sus títulos de defensores de los derechos fundamentales[49].

Este último episodio demuestra hasta qué punto importa la función vigilante de los Tribunales Constitucionales en la deriva del proceso de integración europea, pues de ellos depende que el Tribunal de Justicia imprima en el Derecho de la Unión la sensibilidad constitucional que todavía hoy le resulta un tanto extraña.

En definitiva, la encrucijada en la que se encuentra la protección de los datos personales es la misma en la que debe decidirse el camino que ha de seguir Europa y –con ella o contra ella– la defensa de la libertad de sus ciudadanos.

46. *Google Spain y Google* (C-131/12, EU:C:2014:317).
47. *Melloni* (C-399/11, EU:C:2013:107).
48. Sentencia de 8 de septiembre de 2015, *Taricco y otros* (C-105/14, EU:C:2015:555).
49. Sentencia de 5 de diciembre de 2017, *M.A.S. y M.B.* (C-42/17, EU:C:2017:936), también conocida como *Taricco II*, en la que el Tribunal de Justicia hace suyos los reparos de la Corte Constitucional italiana a su primer pronunciamiento.

3

DERECHO E INNOVACIÓN. PRIVACIDAD Y OTROS DERECHOS EN LA SOCIEDAD DIGITAL[1]

JOSÉ LUIS PIÑAR MAÑAS
Catedrático de Derecho Administrativo.
Universidad CEU-San Pablo de Madrid

3.1. INTRODUCCIÓN

El avance tecnológico plantea retos innegables que afectan a los derechos y libertades de la persona. No es la primera vez que el Derecho se enfrenta a situaciones disruptivas, pero quizá sí nos encontremos ante una situación inédita para el ser humano, que ve cómo la innovación tecnológica es capaz de generar situaciones que van más allá de los límites del conocimiento, pues este puede llegar a estar (ya lo está) en situación de generar nuevo conocimiento e incluso capacidad de decisión al margen de la intervención humana. La inteligencia artificial, la robótica, el uso masivo de datos y la dictadura del algoritmo suponen para el jurista un reto no conocido hasta ahora.

1. Agradezco muy de veras la invitación que me ha formulado María Emilia Casas a participar en tan interesante ciclo de conferencias organizado por la Fundación Ramón Areces sobre «El derecho a la protección de datos personales en la sociedad digital». Mi exposición estuvo basada en parte en reflexiones que había ya expuesto en otras ocasiones y que para aquella ocasión actualicé. En particular, en la Lección que tuve ocasión de impartir en el marco de la solemne celebración de la festividad de San Raimundo de Peñafort en la Facultad de Derecho de la Universidad CEU San Pablo de Madrid, el 7 de febrero de 2018; en el artículo «Derecho, ética a innovación tecnológica», publicado en la *Revista española de Derecho Administrativo*, nº 195, octubre-diciembre 2018, pp. 11–30; «Identidad y persona en la sociedad digital», publicado en De la Quadra Salcedo y Piñar Mañas (Directores), *Sociedad Digital y Derecho*, Ministerio de Industria, Comercio y Turismo, Red. Es, Boletín Oficial Del Estado, Madrid, 2018, pp. 95-111; «¿Qué regulación de los derechos en la sociedad digital?», *Revista Derecho Digital e Innovación*, nº 1, primer trimestre 2019. Lo he actualizado con ciertas referencias posteriores a la fecha de la conferencia (11 de junio de 2019), algunas de las cuales las he recogido también en «Los peligros de una república digital desbocada. A propósito del Real Decreto-Ley 14/2019, de 31 de octubre, en materia de administración digital, contratación del sector público y telecomunicaciones», en *Revista Derecho Digital e Innovación*, nº 3, tercer trimestre 2019. Los trabajos se han realizado en el marco del Proyecto de Investigación DER2016- 79819- R, del Programa estatal de investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, del Ministerio de Economía y Competitividad, sobre «Protección de datos, seguridad e innovación: retos en un mundo global tras el Reglamento Europeo de Protección de Datos», del que soy investigador principal.

En una *law-saturated society* (como recordó Rodotà) ¿qué papel debe jugar el Derecho? ¿Es necesaria nueva regulación para la sociedad digital? ¿Es necesario reformar la Constitución para la efectividad de los derechos en la sociedad digital? ¿Cómo se consigue una regulación que resista a la obsolescencia ante la imparable e imprevisible innovación tecnológica? Seguramente hemos de diseñar un nuevo derecho en el que se vuelva a los principios y se produzca una inevitable relación entre regulación y autorregulación, desde una perspectiva, además, incuestionablemente global.

En este escenario, los derechos deben salir fortalecidos, no debilitados. La dignidad, el libre desarrollo de la personalidad, la libertad y la igualdad frente a los avances de la técnica (con especial referencia a Internet), el derecho a la identidad y la privacidad deben reivindicarse con mayor intensidad que nunca, pues nunca antes habían estado expuestos a las amenazas que ahora se ciernen sobre ellos. Todo ello desde una perspectiva que no admite discusión: la centralidad de la persona en el diseño de lo que podría ser el nuevo derecho de la sociedad digital.

¿Cuántas veces se dice que el Derecho no es capaz de seguir el ritmo de la técnica y que irremediablemente está condenado a ir por detrás de los avances de la innovación tecnológica sin llegar a resolver a tiempo y adecuadamente los problemas de todo tipo que esta plantea? Problemas que afectan sin duda a los derechos fundamentales y muy particularmente a la protección de datos, que parecería que en un nuevo entorno, el de la sociedad digital, no aciertan a encontrar el nivel de tutela o garantía que requieren[2]. Como expondré a continuación, creo sin embargo que, pese a que los retos son innumerables e innegables, todavía estamos a tiempo de que el Derecho ofrezca respuestas frente al avance de la técnica. Lo que ocurre es que seguramente hemos de cambiar ciertos planteamientos acerca de cómo puede o debe configurarse (principalmente desde el punto de vista normativo) y actuar. No creo que sea necesario hablar de un nuevo Derecho para la sociedad digital, pero sí de un nuevo enfoque[3].

Pues bien, en este escenario, ¿qué papel ha de jugar –o puede jugar– el Derecho? En una *law-saturated society* (como recordó Rodotà[4]) seguramente hemos de diseñar un nuevo derecho en el que se vuelva a los principios y se produzca una inevitable relación entre regulación y autorregulación, desde una perspectiva, además, incuestionablemente global y en el que por supuesto los derechos salgan en su caso fortalecidos, nunca debilitados. La dignidad, el libre desarrollo de la personalidad, la libertad y la igualdad frente a los avances de la técnica (con especial referencia a Internet), el derecho a la identidad y la privacidad deben reivindicarse con mayor intensidad que nunca, pues nunca antes habían estado expuestos a las amenazas que ahora se ciernen sobre ellos. Todo ello desde una perspectiva que no admite discusión: la centralidad de la persona en el diseño de lo que podría ser el nuevo derecho de la sociedad digital.

---

2. Sobre ello en general vid. en De la Quadra Salcedo y Piñar Mañas (Directores), *Sociedad Digital y Derecho*, Ministerio de Industria, Comercio y Turismo, Red.Es, Boletín Oficial Del Estado, Madrid, 2018. Accesible en: https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUBNT-2018-97&tipo=L&modo=2
3. Como expuse en la charla que sobre «Sociedad digital: ¿un nuevo escenario para un nuevo derecho» tuve ocasión de impartir en el Seminario Permanente de Derecho Privado organizado por la Universidad de la Rioja y el Centro de Estudios Registrales de La Rioja, el 21 de octubre de 2019.
4. *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, p. 25.

3.2. DERECHO, INNOVACIÓN Y DISRUPCIÓN

Desde luego, no es la primera vez que el Derecho se enfrenta a situaciones disruptivas. Aunque quizá sí nos encontremos ahora ante una situación inédita para el ser humano, que ve cómo la innovación tecnológica es capaz de generar situaciones que van más allá de los límites del conocimiento. La inteligencia artificial[5], la robótica[6], el uso masivo de datos[7], la que se ha venido en llamar dictadura del algoritmo[8], la amenaza creciente para la privacidad o la posible distinción entre identidad física e identidad digital[9], suponen para el jurista retos no conocidos hasta ahora.

En este entorno, en el que se habla ya de la sociedad digital[10], de la persona digital[11], la cuestión es si la innovación digital requiere una nueva y específica regulación de los llamados derechos digitales o, por el contrario, la regulación de los derechos fundamentales es capaz de extenderse y adaptarse a la realidad digital, sin que sea por tanto precisa una nueva regulación.

Ejemplos de una regulación específica en ese sentido ya existen. Sin ir más lejos, entre nosotros, es obligada la referencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales que incluye un Título X, artículo 79 a 97, sobre «Garantía de los Derechos Digitales». Asimismo, la ley brasileña 12.965, de 23 de abril de 2014, por la que se establecen los princi-

---

5. El tema de la inteligencia artificial no es nuevo para el derecho. Véase si no, VV. AA., *Segunda Reunión sobre Inteligencia Artificial y Derecho: comunicaciones. Logroño, 14 de junio de 1991*, editado por la Universidad de Zaragoza, 1991. Más recientemente Susana Navas Navarro y otros, *Inteligencia artificial Tecnología Derecho (Derecho y Tic's)*, Tirant Lo Blanch, Valencia, 2017; Andrea Ottolia y M. Marzetti *Derecho, big data e inteligencia artificial*, Tirant Lo Blanch, Valencia, 2018. Con un alcance más sectorial, José Ignacio Solar Cayón, *La inteligencia artificial jurídica*, Aranzadi, 2018; Jordi Nieva Fenoll, *Inteligencia artificial y proceso judicial (Proceso y Derecho)*, Pons, Madrid, 2018; Cristina Alonso Suárez y otros, *Nuevos desafíos para el derecho de autor: Robótica, inteligencia artificial, tecnología*, REUS, Madrid, 2019; Alessandro Mantelero «Data processing and the risks of Artificial Intelligence», en *Revista Derecho Digital e Innovación*, nº 1, primer trimestre 2019.
6. Por todos vid. Jesús R. Mercader Uguina *El futuro del trabajo en la era de la digitalización y la robótica*, Tirant lo Blanch, 2017 Moisés Barrio Andrés, *Derecho de los Robots*, La Ley Wolters Kluwer, Madrid, 2ª Ed. 2019. Asimismo, José Ignacio López Sánchez, María Amparo Grau Ruiz y María Yolanda Sánchez-Urán Azaña «The impact of robotics and computerization on the labour market: Inclusive insight from a Law and Economics perspective», en *Revista Derecho Digital e Innovación*, nº 3, tercer trimestre 2019.
7. Vid Wolfgang Hoffmann-Riem, *Big Data. Desafíos también para el Derecho*, Civitas, Madrid, 2016; Javier Puyol, *Aproximación Jurídica y Económica al Big Data*, Tirant Lo Blanch, Valencia, 2015; Apol·lònia Martínez Nadal, *Big Data, Cloud Computing y otros retos jurídicos planteados por las tecnologías emergentes*, Aranzadi, 2019. De gran interés, Dwight Steward y Roberto Cavazos, *Big Data Analytics in U.S. Courts: Uses, Challenges, and Implications*, Palgrave Macmillan, 2019.
8. Vid. Taina Bucher, *IF ...THEN. Algorithmic Power and Policy*, Oxford University Press, Oxford, 2018.
9. Distinción esta que es muy reciente. Anthony APPIAH, por ejemplo no se refiere a ello en su importante obra *The Ethics of Identity*, Princeton University Press, Princeton, 2005.
10. Vid. por ejemplo Quadra-Salcedo y Piñar Mañas (directores), *Sociedad Digital y Derecho*, Ediciones del BOE, Madrid, 2018.
11. Como indica Rodotà (*Antropologia del homo dingus*, lección magistral con ocasión de su nombramiento como Doctor Honoris Causa de la Universidad de Macerata, Ed. Bienmegraf, Macerta, 2010, p. 71), la expresión «digital person» se debe a R. Clarke, «The digital person and its application to data surveillance», en *Information Society*, 1994, pp. 77 y ss. Vid. también Daniel J. SOLOVE, *The digital person. Technology and privacy in the Information Age*, New York University Press, 2004.

pios, garantías, derechos y deberes para el uso de Internet en Brasil (*Marco Civil*) o la Ley francesa n° 2016-1321 de 7 de octubre de 2016 *pour une République numérique*. Por otra parte, son numerosas las iniciativas y propuestas elaboradas desde la Sociedad civil en relación con los derechos en la sociedad digital[12].

Que el derecho es capaz de adaptarse a las nuevas realidades es obvio. Sin que sea siempre necesario, además, llevar a cabo una modificación de las normas. En no pocas ocasiones pueden admitir una interpretación que permita adaptarlas a las nuevas realidades. No otra cosa sucedió con el artículo 18.4 de la Constitución, que al establecer que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» encerraba ya un nuevo y autónomo derecho, cual es el derecho a la protección de datos, tal como terminó por afirmar el Tribunal Constitucional en su conocida Sentencia 292/2000, de 30 de noviembre. En Alemania, el Tribunal Constitucional Federal en su Sentencia de 27 de febrero de 2008, ya advirtió que la protección de datos se extiende a los dispositivos de tratamiento de datos. Es decir, el derecho a la privacidad alcanza también a los dispositivos que utilizamos y que forman parte ya de nuestra propia vida, que contienen información que nos identifica y que puede dar una imagen de nuestra personalidad. Es este, pues, un paso de gigante en la evolución del derecho a la privacidad y a la protección de datos, que puede y debe interpretarse de forma extensiva cuando el avance de la sociedad digital así lo requiere. Esta Sentencia nos sitúa en el centro del debate: si con su pronunciamiento el Tribunal Constitucional Alemán ha extendido el derecho a la protección de datos también a los dispositivos que todos utilizamos en nuestra vida cotidiana y que pasan a ser una suerte de extensión de nuestra persona, ¿no es posible hacer lo propio con otros derechos que, reconocidos en la Constitución, pueden también considerarse reconocidos en la sociedad digital sin necesidad de forzar la Constitución?

12. A ello me he referido en «Qué regulación de los derechos en la sociedad digital», op. cit.

En mi opinión resulta evidente que la Constitución de 1978 admite, sin duda, una interpretación que permita extender el reconocimiento de los derechos al entorno digital cuando por su naturaleza así lo requieran. Los derechos y libertades reconocidos en el artículo 14 y la Sección Primera del Capítulo Segundo del Título I («De los derechos fundamentales y de las libertades públicas») son sin duda extensibles al entorno digital. Como también, por supuesto, el respeto a la dignidad de la persona (art. 10). Y no pocos de los «principios rectores de la política social y económica» recogidos en el Capítulo Tercero del mismo Título I admiten reconocimiento o protección en el entorno digital. En cualquier caso, opera la cláusula del artículo 9.2., según la cual, como es de sobra sabido, «corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social». Precepto que no tiene porqué limitarse a la efectividad de los derechos en el mundo físico y que se extiende sin duda al entorno digital, en el que los derechos, todos ellos, han de ser igualmente reales y efectivos. En esta línea se mueve el artículo 79 de la Ley Orgánica 3/2018, que teniendo como enunciado «Los derechos en la Era digital», señala que «los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación».

3.3. LOS RIESGOS DE UNA SOCIEDAD DIGITAL DESBOCADA

En cualquier caso, la sociedad digital y con ella la innovación que la acompañan pueden generar riesgos que antes difícilmente podían ni imaginarse y que son tan posibles como reales. Riesgos que, precisamente por moverse en el entorno digital, no siempre son fáciles de detectar. No me refiero a los ciberataques que constantemente están produciéndose, sino a las posibilidades que tiene la innovación invisible que se desarrolla en el mundo virtual y que puede ser especialmente grave para los derechos fundamentales.

Un ejemplo de lo que ahora expongo es la que se ha venido en llamar República Digital catalana. Como ya he expuesto en otra ocasión[13], hace tiempo que el Gobierno de la Generalidad de Cataluña viene hablando y trabajando en la implantación de una llamada «República Digital» previa a la real[14].

Ya he dicho más veces[15] que nada hay que objetar a la utilización de las posibilidades que ofrece la innovación tecnológica en la llamada era digital para mejorar las condiciones de vida de las personas, el entorno en que vivimos y en definitiva el disfrute y garantía de los derechos fundamentales. Pero estos derechos, en ningún caso, deben sufrir ante el avance tecnológico. Tomás De la Quadra-Salcedo ha advertido que «será desde los derechos fundamentales –desde todos ellos incluido el

13. «Los peligros de una República Digital desbocada...», op. cit.
14. https://www.elperiodico.com/es/politica/20180818/el-govern-apuesta-por-una-republica-digital-previa-a-la-real-6994082
15. «Los peligros de una República Digital desbocada...», op. cit.

de participación política– desde donde debamos reconstruir y articular las tecnologías convergentes con la sociedad del futuro»[16]. Pérez Luño ha señalado que constituye «un problema nodal» de nuestro tiempo «el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades»[17].

Los riesgos son, como digo, reales, no ficticios, y frente a ellos ha de reaccionar el Derecho. Para hacer frente a situaciones semejantes a la iniciativa de la Generalidad, el Gobierno ha aprobado el Real Decreto Ley 14/2019, de 31 de octubre, en materia de administración digital, contratación del sector público y telecomunicaciones. No puedo entrar ahora en su análisis[18]. En mi opinión, la reiterada República Digital está asentada en premisas notablemente contrarias al derecho a la protección de datos y, en particular, al Reglamento (UE) 2016/679, pero quizá algunas de las medidas que prevé el Decreto Ley pueden ser asimismo contrarias al Reglamento y, lo que es peor, a ciertos derechos y libertades.

El de la reiterada república digital es un ejemplo de iniciativas claramente contrarias al derecho a la protección de datos que en lo esencial pasan desapercibidas para los ciudadanos pero que no por ello son menos invasivas de sus derechos; y de una reacción en ciertos aspectos desmedida que pone de manifiesto la dificultad que en numerosas ocasiones tiene el Derecho para enfrentarse a situaciones difíciles incluso de constatar por cuanto se mueven en el mundo virtual.

3.4. EL NECESARIO RECONOCIMIENTO DE ALGUNOS NUEVOS DERECHOS

Algún autor autorizado considera necesario incluir el reconocimiento de los derechos digitales en una hipotética y futura reforma constitucional[19]. Algo que por lo demás es totalmente lógico, pues si se optase por reformar la Constitución es evidente que debería actualizarse el texto para adaptarlo al entorno digital, pero teniendo en cuenta, como luego diré, que cualquier texto que pretendiese abordarse, constitucional o legal, debe poder enfrentarse a cualquier posible innovación que lo hiciese devenir obsoleto. Con otras palabras, quizá el problema no es tanto adaptar la norma a lo digital (que puede no ser el entorno futuro) sino a la entidad sustancial de los derechos fundamentales sea cual sea el entorno en que han de reconocerse y hacerse efectivos.

Así las cosas, sin embargo, cabe pensar, y así es, que ciertos derechos requieran una regulación actualizada o esclarecedora de su contenido y alcance en la sociedad digital. Tal sería el caso, por ejemplo, del derecho de acceso a Internet o el derecho de acceso al conocimiento. Pero sobre todo, como luego veremos, es necesario poner el acento en al menos dos cuestiones de indudable relevancia: cómo la sociedad

16. «Derechos fundamentales, democracia y mercado en la edad digital», en *Derecho Digital e innovación*, nº 2 (abril junio-2019), p. 13 de la edición impresa.
17. «Las generaciones de derechos humanos ante el desafío posthumanista», en De la Quadra-Salcedo y Piñar Mañas (dirs.) *Sociedad Digital y Derecho*, Ediciones del BOE, Madrid, 2018, p. 147.
18. Me remito al análisis urgente del contenido del Decreto Ley que he adelantado en «Los peligros ...»,op.cit.
19. Por todos, Rallo Lombarte: «Una hipotética reforma de la Constitución debería incluir la actualización de la Constitución a la era digital y constitucionalizar una nueva generación de derechos digitales»: «De la "libertad informática" a la constitucionalización de nuevos derechos digitales (1978-2018)», en *UNED. Revista de Derecho Político*, nº 100, septiembre-diciembre 2017, p. 666.

digital puede poner en riesgo el derecho a la privacidad y el modo en que el derecho a la identidad puede resultar condicionado en el entorno digital.

En cuanto al derecho de acceso a Internet[20], ya he señalado en otra ocasión[21] que se trata de reconocerlo como nuevo derecho que además condiciona cada vez más el ejercicio de otros derechos, como el propio derecho a la libertad de circulación, el derecho a la educación y a la cultura, la libertad de expresión e información, incluso el derecho de acceso a la justicia y derecho a la defensa. Pocos derechos pueden ser hoy ajenos a Internet. En este sentido es muy destacable que el artículo 81 de la Ley Orgánica 3/2018 haya reconocido el derecho de acceso universal a Internet independientemente de la condición personal, social, económica o geográfica de las personas[22].

Por otra parte, ante la realidad y alcance de lo que supone el entorno digital, ¿debería reconocerse el derecho al libre acceso al conocimiento en general y al científico en particular? En mi opinión, así debería ser cuando menos en relación con el conocimiento generado con financiación y/o recursos públicos. En otras ocasiones he advertido que la cuestión plantea enormes problemas (por ejemplo de propiedad intelectual o derechos de autor) que no pueden ignorarse, pero se trata de un derecho que en ningún caso puede obviarse. De hecho ya hay iniciativas concretas que van en esa línea. Así, el BOE ha puesto ya en marcha una interesante Biblioteca

20. Sobre ello vid. entre otros, García Mexia, Pablo, «El derecho de acceso a Internet», en Quadra-Salcedo y Piñar (directores), *Sociedad Digital y Derecho*, op.cit., pp. 397 y ss.
21. «Derecho, ética e innovación tecnológica», op. cit, p. 25.
22. Dispone el citado artículo: «1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica. / 2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población. / 3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral. / 4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores. / 5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales. / 6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales».

Jurídica Digital[23] y el Consejo General de la Abogacía Española está impulsando el proyecto de una Biblioteca Digital, como uno de los objetivos de su Plan Estratégico Abogacía 2020 para fomentar la cultura jurídica de calidad y el principio de igualdad de armas en el proceso[24]. Por su parte, los buscadores llevan a cabo una labor espectacular y ahora irrenunciable para facilitar el acceso al conocimiento. No sólo los más conocidos, sino también otros que facilitan el acceso a numerosas publicaciones científicas[25]. En otro ámbito, la iniciativa de la Khan Academy[26] pretende extender de forma gratuita el conocimiento con alcance global y a muy distintos niveles aprovechando las posibilidades que ofrece Internet, con casi 100 millones de usuarios en más de 30 países[27].

En Francia la *Loi pour une République numérique*, ha puesto sobre la mesa el debate sobre el reconocimiento del derecho de acceso al conocimiento[28]. Su artículo 30 añade un nuevo artículo L 533-4 al *Code de la Recherche*[29] que permite la puesta a disposición de los resultas de investigaciones financiadas al menos en un 50% con fondos públicos.

---

23. https://www.boe.es/publicaciones/biblioteca_juridica/
24. Dentro del Eje 1, *Una Abogacía Confiable y Preparada*, de dicho Plan, se ha incluido la creación de «una biblioteca digital intercolegial excelente, que asegure la igualdad de armas en el proceso por medio de un igual acceso a las fuentes de información».
25. Por ejemplo, Teseo (Consulta de la base de datos de Tesis Doctorales), Dialnet, Open Access Theses and Dissertations, Tesis Doctorales en Red, Networked Digital Library of Theses and Dissertations (NDLTD), DART, etc.
26. https://es.khanacademy.org/
27. Salman Khan, creador de la Academia, y la propia plataforma, obtuvieron el premio Princesa de Asturias 2019. En su discurso, el premiado señaló que la Academia pretendía hacer realidad «un mundo donde cada niño verdaderamente tenga acceso a una educación de calidad y gratuita».
28. Vid. Direction de l'Information Scientifique et Technique –CNRS, *Livre Blanc. Une Science Ouverte Dans une République Numérique*, OpenEdition Press, Marsella, 2016, y *Livre Blanc. Une Science Ouverte Dans une République Numérique. Guide Stratégique*, OpenEdition Press, Marsella, 2017. De ambas publicaciones hay también versión en inglés: https://books.openedition.org/oep/1547
29. El *Code de la Recherche* se adoptó en 2004 en base a la *Ordonnance* n° 2004-545 de 11 de junio de 2004. Su nuevo Art. L. 533-4 dispone: «I. 1. Cuando un documento científico resultante de una actividad de investigación financiada al menos en un 50% por subvenciones del Estado, de las colectividades locales o de instituciones públicas, por subvenciones de organismos nacionales de financiación o por fondos de la Unión Europea se publique en una revista publicada al menos una vez al año, su autor dispondrá, incluso después de haber concedido derechos exclusivos a una editorial, el derecho a poner a disposición gratuitamente en formato abierto, por medios digitales, previo acuerdo de los coautores, la versión final de su manuscrito aceptada para su publicación, a condición de que el propio editor la ponga a disposición gratuitamente por medios digitales o, en su defecto, al término de un período que comenzará a contar a partir de la fecha de la primera publicación. Este período es de un máximo de seis meses para una publicación en el campo de la ciencia, la tecnología y la medicina y de doce meses para una publicación en las ciencias humanas y sociales.
    La versión puesta a disposición de conformidad con el párrafo primero no podrá utilizarse en el contexto de una actividad editorial comercial. II. Cuando los datos resultantes de una actividad de investigación financiada al menos en un 50% por el Estado, las autoridades regionales o locales, las instituciones públicas, las subvenciones de los organismos nacionales de financiación o los fondos de la Unión Europea no estén protegidos por un derecho o un reglamento específico y hayan sido hechos públicos por el investigador, la institución o el organismo de investigación, su reutilización será gratuita. III. El editor de un artículo científico mencionado en [el apartado] I no puede limitar la reutilización de los datos de investigación hechos públicos en el contexto de su publicación. IV. Las disposiciones de este artículo son de orden público y cualquier cláusula contraria a ellas se considerará no escrita».

3.5. DERECHO A LA PRIVACIDAD EN LA SOCIEDAD DIGITAL

No creo que sea necesario reiterar una vez más que la privacidad y el derecho a la protección de datos pueden resultar especialmente afectados por la implantación de la sociedad digital. Nada nuevo supone afirmar que la innovación tecnológica implica nuevos y numerosos retos para la protección de datos dado que aquella se fundamenta, entre otras bases, en la posibilidad de tratar masivamente datos de carácter personal. Pero sí creo oportuno hacer referencia a una reciente e importante sentencia del Tribunal Constitucional que ha vuelto a resaltar la importancia de tal derecho. Me refiero a la Sentencia de 22 de mayo de 2019, por la que se ha anulado el apartado 1 del nuevo artículo 58. bis de la Ley Orgánica 5/1985 del régimen electoral general, introducido por la Ley Orgánica 3/2018. Dicho apartado disponía que «La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas». Es decir, se permitía a los partidos políticos recabar datos personales de cualquier fuente (internet, redes sociales, páginas web, tratamientos no automatizados...) con el fin de perfilar a las personas en función de sus opiniones políticas, y todo ello sin el consentimiento de las personas afectadas. Dicha previsión no se encontraba en el proyecto de ley que el Gobierno remitió al Congreso en noviembre de 2017, sino que se introdujo a través de la enmienda nº 331 presentada por el Grupo Parlamentario Socialista en el Congreso de los Diputados durante la tramitación parlamentaria de la Ley. Hay que decir que el texto final fue aprobado por unanimidad de todos los diputados.

Es importante traer a colación esta sentencia porque en ella se hace frente a un supuesto vinculado al tratamiento de datos en la sociedad digital, pues el precepto anulado por el Tribunal Constitucional estaba pensado claramente en la posibilidad que pretendían los partidos políticos de recabar datos de internet, ámbito en el que el control de los datos por parte de sus titulares es mucho más complejo. Y el Tribunal reafirma contundentemente la plena vigencia del derecho a la protección de datos.

Sin entrar en el detalle de la Sentencia, que he analizado en otro lugar[30], sí debe resaltarse que el Tribunal Constitucional comienza identificando «el núcleo de la controversia» que no es otro que el relativo a la violación de los artículos 18.4 y 53.1 de la Constitución, es decir, la violación del derecho constitucional a la protección de datos y la del principio de reserva de ley. En palabras del Tribunal (Fundamento Jurídico –FJ– segundo): «El enjuiciamiento constitucional que nos demanda la impugnación central se circunscribe, pues, a resolver si el legislador ha vulnerado la reserva de ley y el contenido esencial del derecho fundamental a la protección de datos personales (art. 18.4 de la CE en conexión con el art. 53. l CE), por renunciar a establecer el marco en el que se habilita el tratamiento, la finalidad del mismo y las garantías adecuadas frente al concreto uso de la informática previsto en la norma impugnada». En mi opinión, lo que seguramente busca el Tribunal, al concretar desde el principio cuál es el «núcleo de la controversia» o «impugnación central», es dejar claro que no va a basar su va-

30. «El Tribunal Constitucional acaba con la posibilidad de que los partidos políticos recaben sin consentimiento datos sobre opiniones políticas», en la Newsletter del CGAE,10 de junio de 2019: https://www2.abogacia.es/actualidad/opinion-y-analisis/el-tribunal-constitucional-acaba-con-la-posibilidad-de-que-los-partidos-politicos-recaben-sin-consentimiento-datos-sobre-opiniones-politicas/

loración en contrastar el artículo 58. bis de la Looreg con el RGPD sino con la propia Constitución. Y así debe ser. Pues de otro modo el Tribunal se habría enfrentado a una cuestión relativa a la relación entre el derecho nacional y el de la Unión Europea, cuyo análisis no le corresponde y que en su caso habría dado lugar a que el artículo impugnado sería desplazado por el RGPD. Como dice tajantemente el Tribunal (FJ 3): «A este Tribunal le corresponde aplicar la Constitución. Cuando, como ocurre en este proceso, se le demanda el enjuiciamiento constitucional del desarrollo legislativo de un derecho fundamental que se halla en la actualidad parcialmente determinado por el Derecho de la Unión Europea, como es la protección de datos personales, "[l]as exigencias derivadas del Derecho de la Unión no pueden ser irrelevantes a la hora de establecer los márgenes constitucionalmente admisibles de libertad de apreciación política" (STC 1/2012, de 13 de enero, FJ 9). Sin que ello implique de forma alguna que el análisis de constitucionalidad pueda o deba incluir un examen sobre la compatibilidad entre el Reglamento europeo y la ley interna, ni que un eventual juicio de incompatibilidad pueda derivar en la declaración de inconstitucionalidad de una ley interna por oposición a una disposición de Derecho de la Unión, pues cualquier análisis de compatibilidad entre el Derecho de la Unión Europea y la Ley Orgánica 3/2018 se dirimirá en términos de legalidad ordinaria y selección del derecho aplicable en un primer término, y no en clave de contradicción con la Constitución de la norma interna eventualmente contraria al Derecho de la Unión (*mutatis mutandis*, STC 140/2018, FJ 6)».

Las anteriores consideraciones son sumamente importantes, no sólo porque el Tribunal centra el debate en términos constitucionales y no de controversia entre el Derecho nacional y el de la Unión Europea, sino porque da por bueno que el derecho a la protección de datos esté regulado en un Reglamento europeo, que va a ser utilizado como parámetro interpretativo del alcance y contenido de dicho derecho tal cual está reconocido en el art. 18.4 de la Constitución. Por ello, en el FJ 4 de la Sentencia se lleva a cabo un análisis pormenorizado de la regulación de las categorías especiales de datos (como son las relativas a las opiniones políticas) en el Reglamento europeo y en la Ley Orgánica.

A partir de aquí, el Tribunal Constitucional analiza «los parámetros de enjuiciamiento que permitan resolver el contenido central de la impugnación: la vulneración por el legislador de la reserva de ley y el contenido esencial del derecho fundamental a la protección de datos personales (art. 18.4 de la CE en conexión con el art. 53.1 de la CE)».

Me centro ahora sólo en el contenido esencial del derecho a la protección de datos. El TC, remitiéndose a la capital STC 292/2000, recuerda que consiste en un «poder de disposición y de control sobre los datos personales» y que tiene «una doble perspectiva»: «El art. 18.4 de la CE no solo "consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona" (SSTC 11/1998, de 13 de enero, FJ 5; 96/2012, FJ 6; y 151/2014, de 25 de septiembre, FJ 7), sino también, como se desprende de su último inciso ("para garantizar [...] el pleno ejercicio de sus derechos"), un derecho instrumental ordenado a la protección de otros derechos fundamentales, esto es, "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" (STC 292/2000, de 30 de septiembre, FJ 5)». El derecho así concebido no tiene carácter absoluto, claro está. Puede estar sujeto a límites, pero estos han de respetar al menos dos requisitos: primero, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas debe responder a un fin constitucionalmente legítimo o encaminarse a la protección o la salvaguarda de un bien constitucionalmente relevante; segundo, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal. Es pues necesario que una ley defina los límites de los derechos y en particular del derecho a la protección de datos. Pero esta ley, para cumplir con el principio de seguridad jurídica, debe cumplir al menos dos exigencias: previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales. Es decir, la ley que limite un derecho fundamental ha de establecer las garantías mínimas exigibles y adecuadas que permitan dicho límite sin menoscabar el contenido esencial del derecho.

La Sentencia del Tribunal es contundente. Y, lo que ahora nos interesa, nos permite reivindicar que lo que en ella se afirma es cabalmente trasladable al entorno digital. No olvidemos que el marco natural en el que el precepto anulado estaba llamado a desenvolverse era sin duda el de Internet y las redes sociales, donde los derechos, y en particular el derecho a la protección de datos, están tan protegidos y tutelados como lo están en el mundo físico. Con el alcance que de nuevo ha recordado el Tribunal Constitucional.

3.6. DERECHO A LA IDENTIDAD Y SOCIEDAD DIGITAL

Dicho lo anterior, otro de los derechos que puede resultar especialmente afectado por la implantación de la sociedad digital es el derecho a la identidad.

Como ya he señalado en otros lugares[31], el de la identidad se ha convertido en un tema especialmente controvertido sobre todo a partir de la irrupción de la innovación tecnológica en el marco de la sociedad digital.

No es fácil encontrar en el ámbito de las normas jurídicas un reconocimiento expreso al derecho a la identidad, configurado como el derecho a ser uno mismo y diferente de los demás. Desde luego no está expresamente reconocido en nuestra

31. *Derecho e innovación tecnológica. Retos de presente y futuro*, CEU Ediciones, Madrid, 2018, pp. 14-15. «Identidad y Persona en la Sociedad Digital», en Quadra Salcedo y Piñar Mañas (Directores), *Sociedad Digital y Derecho*, Ediciones del BOE, Madrid, 2018, pp. 101 y ss.

Constitución. Según el Tribunal Europeo de Derechos Humanos, el derecho a la identidad está reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos (por ejemplo, Sentencia de 28 de enero de 2003, Peck c/ Reino Unido). En su Sentencia 26 de junio de 2014, en los asuntos 65192/11 (Mennesson c/ Francia) y 65941/11 (Labassee c/Francia) el Tribunal recuerda que el derecho a la propia identidad forma parte integral de la noción de vida privada. Advierte además que privar a alguien de su identidad supone privarle de todos sus derechos. Por su parte, el Tribunal Supremo ha señalado que el reconocimiento de la propia identidad forma parte del libre desarrollo de la personalidad (entre otras, STS, Sala 1ª, de 28 de febrero, 6 de marzo o 18 de julio de 2008).

De lo anterior cabría deducir que la identidad es la que es, sin posibilidad de ser alterada. Pero lo cierto es que no es del todo así. En el mundo físico, analógico si se quiere, el ser humano tiene una identidad formal u oficial, pública, que es la que se define a partir de las circunstancias y del entorno público y recognoscible de cada persona. Somos quienes somos en virtud de haber nacido con un determinado sexo (sin perjuicio de lo que luego veremos) en un determinado lugar un determinado momento. Se nos atribuye un nombre y se nos van asignando características que van configurando esa identidad pública u oficial: se nos asigna un nombre y unos apellidos, vivimos en un determinado lugar (nuestra dirección), se nos asigna un número identificativo, ocupamos o no un determinado puesto de trabajo, obtenemos un título... De Castro ya señaló que el nombre es el signo externo de la individualización de la persona[32].

Pero también hay una identidad que se define en función de los elementos que cada uno quiere que se resalten o le definan. Y en este punto la privacidad asume un papel de primera magnitud, pues la privacidad nos permite mantener e incluso reivindicar o hacer valer la identidad que queremos para nosotros o la que realmente tenemos, y que paradójicamente define asimismo la identidad que queremos mostrar hacia fuera. La privacidad permite controlar mi yo y expresar el yo que quiero transmitir a los demás. De modo que debe quedar a la decisión de cada uno compartir o visibilizar más o menos ámbitos de su identidad. Con alguna excepción, como es obvio. Por un lado, el ámbito privado no compartido debe ser lícito para poder resultar intranscendente mantenerlo reservado o no; por otro, las personas de relevancia pública han de ser conscientes de que su ámbito privado, el que define su yo, debe ser forzosamente mucho más limitado que el de quienes no tienen esa relevancia, llegando incluso a existir ámbitos que para el *uomo qualunque* son admisiblemente privados y que para aquellas son no ya admisiblemente sino obligatoriamente públicos. La identidad privada es mucho más limitada en relación con las personas de relevancia pública. Sería fácil ahora citar decisiones de los tribunales que así lo advierten. O recordar cómo el Tribunal de Justicia de la Unión Europea, en su conocida Sentencia de 13 de mayo de 2014, sobre derecho al olvido, obliga a llevar a cabo una ponderación entre el derecho a la protección de datos y el derecho a la libertad de información o de expresión, lo que en la práctica implica valorar, entre otras circunstancias, la relevancia pública del solicitante del olvido para determinar el alcance de la desindexación en que tal derecho consiste.

32. *Derecho de la Persona. Apuntes de Derecho civil español, común y foral*, apuntes de Cátedra editados por la Delegación del SEU de la Facultad de Derecho de la Universidad Complutense, Madrid, 1945, p. 12.

En definitiva, hay o puede haber una tensión entre la identidad pública que nos dan y la privada que nos damos. Y en gran medida la historia ha oscilado entre los intentos del poder por controlar, definir y tergiversar la identidad de las personas y la lucha del ser humano por alcanzar la propia identidad. Los poderes públicos, no siempre dictatoriales, se han valido de la posibilidad de alterar, tergiversar o manipular la identidad de las personas para convertirlas en amigos o enemigos. El nacismo y el estalinismo así lo hicieron. Pero también se pretendió diseñar en Italia una identidad de Pier Paolo Pasolini para, si no justificar, sí desdramatizar e incluso tolerar su muerte, como ha denunciado Rodotà[33].

De modo que la relación entre libre desarrollo de la personalidad y definición de la propia identidad es en mi opinión incuestionable. Lo cual a su vez está íntimamente relacionado con la dignidad de la persona. Por ello es imprescindible que en una sociedad democrática se respete la identidad de la persona y con ello su propia dignidad.

Como ya he señalado en otras ocasiones[34], la democracia implica saber lo menos posible de las circunstancias que configuran la identidad de las personas. La dictadura, sin embargo, quiere saberlo todo de las personas. Alan Westin ha señalado con acierto que los estados totalitarios prefieren una administración opaca y un ciudadano visible, mientras que las democracias descansan sobre el control a un gobierno transparente y el respeto a la privacidad de la persona[35].

No es de ahora ni nuevo crear identidades totalmente falsas de quien ostenta el poder para impresionar, subyugar, asombrar o fascinar a los súbditos. Las identidades falsas condicionan la relación con el otro. La democracia se basa en que la identidad oficialmente pública esté configurada por los menos elementos posibles, mientras que la privada puede ser tan limitada o tan extensa como cada persona decida

33. En *Pasolini: crónica giudiziaria, persecuzione e morte*, libro coordinado por Laura Betti, Garzanti, Milán, 1977, pp. 279-291. También recogido en Rodotà, *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid 2010, pp. 317 y ss.
34. «Identidad y persona en la sociedad digital», op. cit. Reitero que gran parte de las reflexiones que ahora expongo ya las había transmitido con anterioridad.
35. *Privacy and Freedom*, Atheneum, New York, 1967, p. 23.

sin que por ello puedan derivarse consecuencias negativas para ella. Las dictaduras quieren saber si una persona es homosexual o tiene una determinada ideología; las democracias quieren que las personas puedan dar a conocer que son homosexuales o tienen una determinada ideología sin que para ellas derive de ello consecuencia alguna. Las dictaduras quieren heterodefinir la identidad de las personas y decidir las consecuencias que de ello derivan; las democracias quieren permitir que cada uno defina su propia identidad sin que de ello deriven consecuencias. El Tribunal Constitucional Federal Alemán ha declarado, mediante sentencia de 10 de octubre de 2017[36], que es inconstitucional la imposibilidad de inscribir a una persona con un tercer sexo diferente al masculino o femenino. La Sentencia es de extraordinaria importancia para el derecho a la identidad. El Tribunal llama la atención acerca de la importancia de la identidad de género en la vida cotidiana: «La identidad de género desempeña un papel importante en la vida cotidiana: en parte, el género determina los derechos y obligaciones previstos por la ley; además, a menudo constituye la base para la identificación de una persona, y la identidad de género también es importante en la vida cotidiana, independientemente de las disposiciones legales. En gran medida, determina, por ejemplo, cómo se visten las personas o qué se espera de una persona en términos de su apariencia, educación o comportamiento»[37]. Y la importancia que la propia identidad tiene para el libre desarrollo de la personalidad: la Ley Fundamental de Bonn también «protege la identidad de género de las personas a las que no se les puede asignar ni el género masculino ni el femenino. Estas personas podrían desarrollar su personalidad más libremente si se atribuyera menos importancia a la asignación de género en general... La asignación de género es un factor particularmente relevante sobre cómo perciben las personas los demás y cómo ven su propia personalidad»[38]. Y resalta la importancia que tiene en la construcción de la propia identidad: «el reconocimiento del género en la ley del estado civil tiene un efecto de creación de identidad... ; define los aspectos centrales de la identidad legalmente relevante de una persona»[39]. En definitiva, la identidad propia, la real en una democracia, no la que atribuye tasadamente la ley, es parte esencial del libre desarrollo de la personalidad y de la dignidad humana. La identidad en definitiva condiciona la vida misma de la persona, su quehacer cotidiano. Su desarrollo normal y tranquilo como persona[40].

La Sala Primera de nuestro Tribunal Supremo, ya a partir de la Sentencia 929/2007, de 17 de septiembre, dejó de exigir la operación quirúrgica de reasignación sexual para admitir la pretensión de rectificación de la mención del sexo y el nombre en la inscripción de nacimiento en el Registro Civil. Algo que ha reiterado en las Sentencias 158/2008, de 28 de febrero, 182/2008, de 6 de marzo, 183/2008, de 6 de marzo, 731/2008, de 18 de julio y 465/2009, de 22 de junio[41]. En todas las sen-

36. http://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2017/10/rs20171010_1bvr201916en.pdf?__blob=publicationFile&v=1
37. Epígrafe (39).
38. Epígrafe (40).
39. Epígrafe (47).
40. Ya existen formularios en los que se incluyen campos no para expresar el sexo de una persona, sin más, sino para reflejar «el género con el que me identifico».
41. Así lo Recuerda el Auto de dicha Sala de 10 de marzo de 2016 (recurso 1583/2015) por el que planteó cuestión de inconstitucionalidad en relación al art. 1 de la Ley 3/2007, reguladora de la rectificación registral de la mención relativa al sexo de las personas, por presunta vulneración de los artículos 15 , 18.1 y 43.1, en relación al 10.1, todos ellos de la Constitución, en cuanto

tencias se resalta la importancia de la identidad y su relación con la dignidad de la persona y el libre desarrollo de la personalidad. Como también, tal como ya hemos visto, ha destacado el Tribunal Europeo de Derechos Humanos y el propio Tribunal de Justicia de la Unión Europea[42].

El Tribunal Constitucional, en su notable sentencia 99/2019, de 18 de julio, ha dejado claro el alcance del derecho a la propia identidad en términos muy semejantes a los que acabo de exponer.

La sentencia se dicta como consecuencia de la cuestión de inconstitucionalidad promovida por la Sala de lo Civil del Tribunal Supremo respecto al art. 1.1 de la Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas, por presunta vulneración de los arts. 15, 18.1 y 43.1 de la CE, en relación con el art. 10.1 de la CE. En particular por la imposibilidad de que los menores de edad puedan promover dicha rectificación registral. El Tribunal falla en el sentido de declarar nulo dicho artículo 1.1 «pero únicamente en la medida que incluye en el ámbito subjetivo de la prohibición a los menores de edad con "suficiente madurez" y que se encuentren en una "situación estable de transexualidad"». Para llegar a tal conclusión, el Tribunal lleva a cabo un pormenorizado estudio del principio de proporcionalidad, el principio constitucional del libre desarrollo de la personalidad y el derecho a la privacidad y la protección de datos. Me centro en los dos últimos, por la trascendencia que ahora tienen para nosotros.

En mi opinión, la cuestión más relevante que plantea la Sentencia es la relación entre libre desarrollo de la personalidad, identidad y dignidad de la persona. En el Fundamento Jurídico 4 de la Sentencia, el Tribunal señala que «la propia identidad, dentro de la cual se inscriben aspectos como el nombre y el sexo, es una cualidad principal de la persona humana. Establecer la propia identidad no es un acto más de la persona, sino una decisión vital, en el sentido que coloca al sujeto en posición de poder desenvolver su propia personalidad. Cualquiera que se vea obligado a vivir a la luz del Derecho conforme a una identidad distinta de la que le es propia sobrelleva un lastre que le condiciona de un modo muy notable en cuanto a la capacidad para conformar su personalidad característica y respecto a la posibilidad efectiva de entablar relaciones con otras personas». Recuerda que el Tribunal Europeo de Derechos Humanos reconoce un «derecho a la autodeterminación» de la propia identidad, de modo que «la libertad de decidir la propia identidad sexual es uno de los elementos esenciales más básicos», que el Tribunal Federal alemán ha reconocido el «derecho general a la propia personalidad» y que nuestro Tribunal Supremo, en base al libre desarrollo de la personalidad, ha dado prevalencia en la determinación del sexo a los factores psicosociales frente a los biológicos. Expuesto lo anterior, el Tribunal Constitucional asume que la «determinación autónoma de la propia identidad» está vinculada con «el libre desarrollo de la personalidad». Y añade que el hecho de no permitir que un menor de edad pueda obtener la rectificación registral de la mención del sexo, supone que a los menores se les priva de la eficacia del principio constitucional del libre desarrollo de la personalidad en lo que se refiere a decidir acerca de la propia identidad, lo cual «incide de un modo principal en su dignidad como

---

que solo reconoce legitimación a las personas mayores de edad para solicitar la rectificación de la mención registral del sexo y del nombre. Dicha cuestión ha sido resuelta por Sentencia 99/2019, de 18 de julio, a la que luego me refiero en el texto.

42. El Auto de 10 de marzo de 2016, citado en la nota anterior, incluye un muy completo análisis de la jurisprudencia de ambos tribunales.

tal individuo, cuya salvaguarda es la justificación última de un Estado constitucional como el establecido en la Constitución de 1978».

En cuanto a la relación entre identidad e intimidad, el Tribunal, siempre en el Fundamento Jurídico 4, recuerda su doctrina previa según la cual «el derecho a la intimidad personal del art. 18 de la CE implica "la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana" (STC 231/1988, de 2 de diciembre, FJ 3)». Y a ello se ha añadido que «lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio (SSTC 127/2003, de 30 de junio, FJ 7, y 89/2006, de 27 de marzo, FJ 5)».

El Tribunal, aplicando la doctrina reseñada, aprecia que «la falta de equivalencia entre el sexo atribuido al nacer, que es el que accede originariamente al registro civil, y el que un individuo percibe como suyo es una de esas circunstancias particularmente relevantes que la persona tiene derecho a proteger del conocimiento ajeno. Ello se debe a que esa reserva constituye un medio eficaz de que aparezca como único y verdadero sexo el segundo de ellos –el percibido por el sujeto– y, en consecuencia, no trascienda al conocimiento público su condición de transexual».

Cierto que el Tribunal se refiere en este caso a la identidad de género, pero no cabe duda de que sus conclusiones son aplicables al concepto mismo de identidad y a la relación que tiene con el libre desarrollo de la personalidad, la dignidad de la persona y su intimidad. Algo que por lo demás ha de operar de acuerdo a criterios exactamente iguales en el ámbito de la sociedad digital. Lo que plantea el tema de la definición y control de la propia identidad en dicho ámbito.

En el entorno digital confluyen elementos que configuran tanto la identidad que cada uno quiere o pretende darse en ejercicio del principio de libre desarrollo de la personalidad, como la que se otorga. Lo que ocurre es que en el entorno digital la heteroformación de la identidad depende de factores que no siempre operan en el mundo físico o lo hacen de un modo muy diverso. Pues en el entorno digital las posibilidades de conformar desde fuera del propio sujeto su identidad y con ello su personalidad son sin duda mucho más numerosas, y cualitativamente diversas.

¿Cómo altera lo digital el concepto de persona y de identidad?. Hoy ya se habla de identidad digital[43], de persona digital[44].

Como ya he señalado en otros lugares[45], la identidad *online* puede llegar a ser definida no desde la autonomía de la persona sino heterónomamente. El poder de los algoritmos puede configurar la identidad de la persona, una identidad controlada, diseñada y vigilada. Lo que pone en cuestión el propio derecho al libre desarrollo de la personalidad. Una identidad cuya configuración puede limitarse en base al modo en que se reconducen e incluso definen los gustos o prioridades

43. Clare Sullivan, *Digital Identity: An Emergent Legal Concept The role and legal nature of digital identity in commercial transactions*, University of Adelaide Press, 2011. Puede consultarse en http://www.jstor.org/stable/10.20851/j.ctt1sq5wqb.1.
44. Daniel J. Solove, *The digital person. Technology and privacy in the Information Age*, New York University Press, 2004.
45. *Derecho e innovación tecnológica. Retos de presente y futuro*, CEU Ediciones, Madrid, 2018, pp. 14-15.; «Identidad y persona en la sociedad digital», op.cit.

de las personas. Se puede perfilar con facilidad a las personas y puede limitarse el marco de su desarrollo personal en un proceso difícil de identificar y ante el que puede resultar aún más difícil resistirse, pues en definitiva la aplicación del algoritmo va a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello deriven. Pero al mismo tiempo puede cercenar la apertura y diversificación de la personalidad y por tanto de la propia identidad, pues en definitiva se va empobreciendo la capacidad de apertura a lo diverso y nuevo. Lo que a largo plazo y de forma casi desapercibida puede llegar a condicionar e incluso definir desde fuera la personalidad del ser humano, que poco a poco pasa a ser más controlable y maleable.

Las anteriores consideraciones nos ponen sobre aviso de algo innegable: la convivencia de un entorno físico y un entorno digital puede dar lugar a una diversidad de identidades, física una, digital otra (u otras). En el futuro digital, en realidad ya hoy, junto a la identidad física convive la identidad virtual, *online*: «en el futuro, la identidad será la materia prima más valiosa para los ciudadanos y esta existirá principalmente *online*» (Schmidt y Cohen[46]). Se ha afirmado asimismo que la identidad es el nuevo dinero[47] y se ha puesto de manifiesto la importancia que para las finanzas tiene la identidad digital[48].

El control sobre la propia identidad en la sociedad digital se pretende fortalecer tecnológicamente con iniciativas tales como el sistema *Self Sovereign Identity*[49], por el que, en base al principio de autodeterminación informativa en relación con los propios datos, y con la participación de diversos actores en el mundo digital puede garantizarse con mayor fiabilidad la identidad de las personas a través sobre todo de la emisión de testimonios relacionados con los atributos que definen la identidad.

---

46. El *futuro Digital*, Ediciones Anaya, Madrid, 2014.
47. Birch, David, *Identity is the New Money*, London Publishing Partnership, Londres, 2014.
48. Foro Económico Mundial, *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity*, 2016. Disponible en: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
49. Vid por ejemplo *Self Sovereign Identity. A guide to privacy for your digital identity with Blockchain*, disponible en: https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

Por otra parte, la gestión de la identidad e incluso su definición misma en la sociedad digital requieren de una incuestionable interrelación entre el Derecho, la Técnica y la Ética.

En primer lugar, el Derecho debe encontrar su lugar en la nueva situación. Como señala Rodotà[50], las nuevas realidades producidas por la ciencia y la tecnología, hacen que la sociedad pida al derecho seguridad, más que protección. Hemos pasado de una época de «valores generalmente compartidos» a una situación de «politeísmo de valores». Aparece una «demanda de certeza a toda costa» y «el derecho acaba tomando tintes autoritarios, representa una imposición y no el reflejo de un sentir común». La frontera entre el derecho y el no-derecho, entre la exigencia de certeza social y la identidad individual se hace evanescente, y se plantea un interrogante capital: «¿cuáles son las áreas en las que puede intervenir legítimamente la norma jurídica? ¿Cuáles son en definitiva los límites del derecho?».

La extensión de esos límites se ha denunciado por muchos, que advierten que el derecho no debe poner puertas al campo, limitar o restringir el avance de la técnica. Y esto sin duda es así, pero tampoco debe abrir o no cerrar la puerta al desalmado. En este sentido, el diálogo entre derecho y técnica se impone. Como ha señalado Lorenzo Martín Retortillo, «la técnica no tiene porqué arrumbar al Derecho»[51], pero este deseo no siempre se cumple. Esteve Pardo ha llegado a decir incluso que «se está estableciendo como una nueva división de poderes entre el poder establecido por la ciencia y el poder establecido por el derecho», de modo que «la ciencia está ocupando extensos territorios tradicionalmente atribuidos al derecho y efectivamente dominados por él hasta tiempos muy recientes»[52]. En cualquier caso, las leyes sólo son posibles si van de la mano de la realidad social y tecnológica, no contra ellas, como ha advertido Marc Langheinrich[53].

Ese diálogo ha de ser, en realidad, un trílogo. Pues además del derecho y la técnica ha de darse voz a la ética. El diálogo entre ética y derecho no es nuevo y nada debo decir ahora sobre ello, pues excedería con mucho el alcance de estas páginas. Sí debo resaltar que, en efecto, el derecho por sí sólo no basta para hacer frente a los retos que el avance tecnológico, que la innovación, trae consigo, y que tanto pueden incidir en la configuración de la identidad digital. En ciertos ámbitos esta perspectiva está ya asumida. Esta es la razón de ser, por ejemplo, de los Comités de Ética en la Investigación[54] o de la aproximación ética a la protección de datos[55].

---

50. *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, p. 12.
51. Martín Retortillo, L., «Presentación», en *La autorización administrativa. La Administración electrónica. La enseñanza del derecho administrativo hoy. Publicaciones de la Asociación Española de Profesores de Derecho Administrativo*, Thomson Aranzadi, Cizur Menor, 2003, p. 10.
52. *Técnica, riesgo y Derecho. Tratamiento del riesgo tecnológico en el Derecho ambiental*, Ariel Derecho, Barcelona, 2009, pp. 99 y 100.
53. «Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems», en la Revista *Ubicomp 2001: Ubiquitous Computing 2001*, pp. 273-291, disponible en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf
54. Ver el muy interesante Documento Canadian Institutes of Health Research, Natural sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research council of Canada (2014), *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*. Disponible en http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf
55. No hace mucho el Supervisor Europeo de Protección de Datos ha creado un *Ethics Advisory Group*. Su Informe 2018 es de extraordinario interés: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

Esta perspectiva ética, este trílogo entre derecho, técnica y ética ha de traducirse también en el protagonismo que los principios han de tener en la regulación jurídica de la innovación y sus consecuencias sobre la identidad en la sociedad digital. En más de una ocasión he señalado[56] que cuanto más novedoso, más concreto, más específico es un tema más hemos de acudir a los principios, al objeto de evitar la obsolescencia del derecho. En una época en que la obsolescencia programada de los objetos y dispositivos es incluso considerada delito, como se ha hecho en Francia (enero de 2018), debe evitarse la del derecho, y para ello debería evitarse hacer girar la regulación en torno a previsiones excesivamente pegadas a la realidad concreta que debe ser regulada. Lo que nos lleva a plantear la trascendencia de los principios generales en la regulación, para cuyo análisis son imprescindibles las aportaciones de mi Maestro, Eduardo García de Enterría[57].

En definitiva, ante la innovación tecnológica hemos de volver a los principios, a lo esencial, pues de otro modo corremos el riesgo de movernos en un escenario cambiante, improvisando soluciones que terminan por quedar obsoletas antes incluso de ser plenamente aplicadas, desbordadas por la evolución, inmisericorde para el derecho, de los avances de la técnica.

Por tanto el derecho, la tecnología y la ética, como antes señalaba, han de ir de la mano para proteger la identidad digital y en consecuencia la dignidad misma de la persona.

El derecho ha de aportar los principios. Como he advertido más atrás, la identidad de la persona se configura hoy en la sociedad digital en torno al tratamiento de datos personales. Por lo que resulta de especial relevancia la aprobación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE: Reglamento general de protección de datos[58], plenamente aplicable desde el 25 de mayo de 2018[59]. Como he señalado en otra ocasión[60], el Reglamento supone la apuesta europea por el máximo respeto a la protección de datos en base al reconocimiento que de tal derecho contiene el artículo 8 de la Carta Europea de los Derechos Fundamentales[61]. Supone el cambio a un nuevo modelo de protección de datos que está llamado a ser la referencia global en protección de datos. No sólo por la influencia que el texto pueda tener en los marcos y desarrollos normativos de no pocos países, sino por la extraordinaria amplitud de su ámbito de aplicación territorial (art. 3.2). Las más grandes empresas multinacionales que basan en el trata-

56. Últimamente en *Derecho e innovación tecnológica…*, op. cit., pp. 16 y ss.
57. *Reflexiones sobre la Ley los principios generales del Derecho*, Civitas, Madrid, 1984, pp. 33-35.
58. DOUE nº L 119, de 4 de mayo de 2016.
59. Sobre el Reglamento, entre otras obras, vid. Piñar Mañas, J.L. (Dir.), Álvarez Caro, M. y Recio Gayo, M. (Coords.) *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Editorial REUS, Madrid 2016; López Calvo, José, *Comentarios al Reglamento Europeo de Protección de Datos*, SEPIN, Madrid, 2017.
60. «Sociedad, innovación y privacidad», en *Información Comercial Española*, nº 897, julio-agosto 2017, pp. 71 y ss.
61. «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

miento de datos gran parte de su actividad (Google, Facebook, Amazon, Microsoft, Linkedin, Yahoo, y tantas otras) van a tener que adaptarse obligatoriamente al nuevo Reglamento Europeo. Ya sólo esta consecuencia es de un alcance y trascendencia hasta ahora desconocidos. Y se inscribe en un proceso de globalización de la protección de datos que va consolidándose sin pausa en los últimos años y que resulta imprescindible para conseguir que la tutela de la protección de datos no se quede en meras palabras o buenas intenciones en la sociedad digital. Que además resulta especialmente protegida, y con ella el control sobre la identidad digital, a través de la definición de principios como el de responsabilidad proactiva, privacidad desde el diseño y privacidad por defecto.

Por otra parte, son de extraordinaria importancia diversas Sentencias del Tribunal de Justicia de la Unión Europea que afectan directamente a grandes multinacionales y que decididamente advierten que la normativa europea de protección de datos tiene un alcance tal que no está dispuesta a que la defensa de la privacidad ceda cuando los tratamientos de datos puedan llevarse a cabo desde fuera de las fronteras europeas. Me refiero a las Sentencias de 13 de mayo de 2014, Asunto C-131/12, *Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González*, en la que, como es sabido, se exige a Google Inc. que atienda el derecho al olvido de una persona que la solicita en España; de 6 de octubre de 2015, asunto C-362/14, *Maximillian Schrems*, por la que se declara inválida la Decisión 2000/520/CE de la Comisión Europea, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro; y de 8 de abril de 2014, asunto C 594/12, *Digital Rights Ireland*, por la que se declara inválida la Directiva 2006/24/CE, de retención de datos. Sentencias todas ellas que nos hacen mantener la esperanza en que el Derecho sigue siendo capaz de tutelar los derechos fundamentales incluso en un escenario de globalización e innovación protagonizado por grandes compañías multinacionales.

3.7. ELEMENTOS QUE CONDICIONAN Y CARACTERIZAN LA REGULACIÓN DE LOS DERECHOS EN LA SOCIEDAD DIGITAL

Dicho lo anterior, y admitiendo que la sociedad digital va a impactar (ya lo está haciendo) especialmente en el derecho a la privacidad y en el derecho a la identidad, haré a continuación una referencia a otras muy importantes cuestiones referidas a la regulación de los derechos en la sociedad digital[62]:

Primero, la posibilidad de un nuevo marco de derechos de la ciudadanía digital –que sin duda ha de ser bienvenida– no puede hacernos perder la verdadera perspectiva de la regulación: siempre ha de estar focalizada hacia la persona sin más, no hacia la persona-digital. Lo digital no es más que un calificativo del sustantivo persona. O dicho de otro modo, lo primero y esencial es reconocer todos los derechos, incluido el derecho a tener derechos[63], a la persona, al ser humano; y a continuación reconocer los derechos a la persona digital. En todo este proceso la centralidad de la persona es clave de bóveda.

62. Reflexiones que ya he expuesto en «Derecho, ética e innovación tecnológica», op.cit.
63. Rodotà, S., *El derecho a tener derechos*, Trotta, Madrid, 2014.

Segundo, cuanto más novedoso, más concreto, más específico es un tema, más hemos de acudir a los principios, al objeto de evitar la obsolescencia del derecho. Y para ello debería evitarse hacer girar la regulación en torno a previsiones excesivamente pegadas a la realidad concreta que debe ser regulada. La norma ha de ser capaz, en efecto, de trascender a la época en que se dicta, sobre todo en momentos como los actuales en los que la innovación hace que un día quede superado por lo que acontece el siguiente. Evitemos que vuelva a tener sentido la famosa denuncia de Julius Von Kirchmann, «tres palabras del legislador convierte bibliotecas enteras en basura»[64].

Buen ejemplo de lo que digo (evitar la obsolescencia de la norma) lo encontramos en el Reglamento general de protección de datos, cuyo artículo 24, pieza clave del nuevo modelo que impone el Reglamento[65], dispone que «teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario». Cáigase en la cuenta de que, en virtud del principio de responsabilidad proactiva, quienes traten datos personales están obligados a adoptar medidas que permitan garantizar y demostrar que se respeta el derecho fundamental a la protección de datos, sea cual sea el estado de la técnica, sea cual sea el momento en que se tratan los datos. Ese precepto es válido ahora y lo será en el futuro, no sólo próximo, sino lejano. Dentro de diez, quince, cincuenta, cien años, una hipotética vigencia

64. *La Jurisprudencia no es ciencia* (trad. Antonio Truyol y Serra), Instituto de Estudios Políticos, Madrid, 1951.
65. Sobre ello vid. Piñar Mañas, J. L. (Dir.), Álvarez Caro, M. y Recio Gayo, M. (Coords.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Editorial REUS, Madrid, 2016.

del citado artículo le permitiría, con idéntica redacción, seguir siendo eficaz para proteger la privacidad, pues sea cual sea la realidad de la técnica, quien trate datos personales deberá respetar el derecho a la protección de datos adoptando para ello, obligatoriamente, las medidas que para entonces sean las adecuadas.

Ejemplo de posible desencuentro entre la regulación general y una regulación más dirigida al entorno digital o cuando menos a un entorno más cercano a las llamadas nuevas tecnologías (pero en cualquier caso demasiado específica) nos la ofrece la tensión entre el citado Reglamento General de Protección de Datos y la propuesta de nuevo Reglamento sobre E-Privacy. No son pocos, entre los que me encuentro, los que consideramos que seguramente los principios del Reglamento General de Protección de Datos pueden dar respuesta a las cuestiones que se plantean en el ámbito de las comunicaciones electrónicas.

La lucha contra la obsolescencia del derecho, en general, y en la sociedad digital, en particular, no solo exige regular en base a principios, sino diseñar un marco normativo en el que convivan la regulación y la autorregulación. No tengo la menor duda de que la innovación y la sociedad digital traen consigo un nuevo sistema de fuentes, cada vez más cercano al modelo anglosajón, en el que la autorregulación tendrá un protagonismo indiscutible. Como ya he señalado en otras ocasiones[66] junto a la regulación de los principios esenciales de la materia regulada y de los elementos formales necesarios para la efectividad de lo regulado (por ejemplo reglas procesales o procedimentales) debe darse paso a la autorregulación por varios motivos: por un lado para permitir la adaptación de la regulación a la realidad del caso concreto, sin la rigidez de la heterorregulación sometida a rigurosos procesos de elaboración y aprobación de la norma; por otro para dar entrada a la participación responsable de los diferentes actores en la regulación del entorno en que operan. Todo ello, por supuesto, dentro de las reglas y principios del estado de derecho y teniendo en cuenta algo esencial: en la definición de los derechos fundamentales no hay lugar para la autorregulación.

Manifestación de la autorregulación son los códigos de conducta, códigos tipo, códigos deontológicos, normas corporativas vinculantes, y otros ejemplos de normas, que lo son en la medida en que incorporen mecanismos para hacerlos vinculantes para quienes los elaboran o se adhieren a ellos. De otro modo estaríamos ante simples declaraciones unilaterales de voluntad sin efectos jurídicos frente a terceros[67] que para nada cumplirían las exigencias de un marco normativo válido para regular relaciones jurídicas.

Como es fácil adivinar, la autorregulación así entendida puede ser cauce adecuado para la regulación de la innovación tecnológica de acuerdo a principios generales válidos, con vocación de permanencia, que son desarrollados por normas heterónomas o autorregulaciones que permiten la adaptación al proceso innovador. Esta nueva forma de regular requiere como elemento imprescindible el compromiso responsable del destinatario de la norma, sea fruto de la regulación o de la autorregulación, como establece el artículo 24 del Reglamento General de Protección de Datos al que acabo de referirme más atrás.

---

66. «Derecho, ética e innovación tecnológica», op. cit. pp. 21-22.
67. Vid Real Pérez (Dir.) *Códigos de conducta y actividad económica. Una perspectiva jurídica*, Pons, Madrid, 2010.

3.8. UNA REFERENCIA A LA REGULACIÓN DE LA GARANTÍA DE LOS DERECHOS DIGITALES EN LA LEY ORGÁNICA 3/2018

La regulación de los derechos en el entorno digital es, en definitiva, una apuesta arriesgada que merecería una reflexión y debate profundos, pues estamos hablando de la regulación del futuro y nuevo Derecho. En España la regulación de las garantías de los derechos digitales, sin embargo, se ha incorporado por vía de enmienda presentada en el Congreso durante la tramitación del Proyecto de Ley Orgánica de Protección de datos Personales[68]. Como ya he señalado en otro lugar[69], durante la tramitación parlamentaria del Proyecto en el Congreso, se produjeron cambios sustanciales en el texto de la norma, de modo que incluso hubo que modificar la propia denominación de la Ley. Como es sabido se incorporó un nuevo Título X que regula la garantía de los derechos digitales, y que hoy forma parte de la Ley Orgánica 3/2018[70]. Desde luego hay que agradecer que el citado Título haya generado a posteriori un notable debate sobre su oportunidad y contenido, con opiniones encontradas. Por mi parte considero que debería haberse planteado un debate más reposado e intenso sobre la opción que finalmente se ha impuesto, sin perjuicio de la bondad de algunos extremos, como el propio reconocimiento del derecho de acceso a Internet, al que ya me he referido.

La Exposición de Motivos de la reiterada Ley Orgánica 3/2018, de 5 de diciembre, de derechos digitales de los ciudadanos señala:

> «Internet, por otra parte, 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. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.
>
> Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

---

68. *Boletín Oficial de las Cortes Generales*, Congreso de los Diputados, XII Legislatura, Serie A, Proyectos de Ley, 18 de abril de 2018, Núm. 13-2.
69. «Estudio Introductorio», en *Código de Protección de Datos*, La Ley-Wolters Kluwer, Madrid, 2018, p. 12.
70. Vid. Rallo, Lombarte, «Del derecho a la protección de datos a la garantía de nuevos derechos digitales», en Rallo Lombarte, Artemi (Director), *Tratado de Protección de Datos*. Tirant lo Blanch, Valencia, 2019, pp. 23 y ss. BARRIO, Moisés, «Garantía de los derechos digitales en la LOPDGDD (Título X)», en López Calvo (coordinador), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Bosch, Wolters Kluwer, Madrid, 2019.

> Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea».

La adición del Título X, artículos 79 a 97, en el que se regula la garantía de los derechos digitales ha sido controvertida. No cabe duda de que fijar las bases de tales garantías es algo digno de ser resaltado. Sin embargo, en mi opinión, quizá no sea la LOPD el lugar más adecuado para su regulación. No sólo porque se desdibuja notablemente el alcance de la Ley Orgánica, que ahora pasa a tener cuando menos un doble objeto (trascendiendo con mucho al RGPD[71]) sino porque seguramente la regulación de los derechos fundamentales en la sociedad digital merece una Ley Orgánica específica que haga honor a la importancia del tema[72], y no un Título de una Ley muy concreta que tiene directa conexión con el artículo 18.4 de la Constitución. Quizá el artículo 1º de la Ley Orgánica en su apartado *b)* pretende justificar la inclusión del nuevo Título X por una pretendida conexión con el citado artículo constitucional, pues señala que también es objeto de la Ley «garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución». Pero lo cierto es que es difícil entender que sea así. De entrada, el artículo 79 de la LOPDGDD va mucho más allá, al disponer que los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Previsión que, como digo, va mucho más allá que el reiterado artículo 18.4.

Además no se llevó a cabo debate alguno ni preparación de la disposición, lo que contrasta por ejemplo con el proceso de elaboración de la Ley sobre la *République Numérique* francesa[73].

Sea como fuere, la Ley regula cuestiones de enorme importancia e interés para el desarrollo de los derechos fundamentales en la sociedad digital. No puedo ahora analizar con detalle los derechos que recoge la Ley, algunos de los cuales, además, son objeto de estudio en esta misma obra, pero sí procede siquiera enumerar los derechos que se recogen: el derecho a la neutralidad de Internet (art. 80), derecho de acceso universal a Internet (art. 81), derecho a la seguridad digital (art. 82), derecho a la educación digital (art. 83), régimen de la protección de los menores en Internet (art. 84) y protección de datos de los menores en Internet (art. 92), derecho de rectificación en Internet (art. 85) y derecho a la actualización de informaciones

71. Digo que tiene cuando menos un doble objeto porque la Ley Orgánica tiene también otras finalidades que la alejan del espíritu inicial del Proyecto de Ley remitido al Congreso.
72. Sobre ello véase Tomás De la Quadra Salcedo y José Luis Piñar (directores), *Sociedad Digital y derechos*, op.cit..
73. Ver la extensa documentación disponible sobre la preparación y aprobación de la ley francesa en http://www.assemblee-nationale.fr/14/dossiers/republique_numerique.asp

en medios de comunicación digitales (art. 86), derecho al olvido en búsquedas de Internet y en servicios de redes sociales y servicios equivalentes (arts. 93 y 94 respectivamente), derecho de portabilidad en servicios de redes sociales y servicios equivalentes (art. 95), derecho al testamento digital (art. 96).

Además, el Título X dedica una especial atención a los derechos digitales en el ámbito laboral[74], y en este sentido regula el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), derecho a la desconexión en el ámbito laboral (art. 88), derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89) el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90) y los derechos digitales en la negociación colectiva (art. 91). En fin, la ley regula las políticas de impulso de los derechos digitales (art. 97).

Como he señalado, el hecho de regular ciertos derechos digitales, o al menos su garantía, no debería plantear grandes críticas. Pero me temo que la «reforma» de la Ley Orgánica de Protección de Datos habría merecido, como antes apuntaba, una más detenida reflexión. Cierto que la «reforma» se asumió en el Congreso por unanimidad de todos los grupos parlamentarios, pero con escaso debate. Lo que ha dado lugar a un Título que, repito, contiene preceptos interesantes (por ejemplo artículos 79 a 83 y 97) pero otros puede que resulten más problemáticos de lo que podría pensarse. De entrada hay preceptos, como los artículos 93 a 95 que parecen establecer regímenes diferentes para derechos similares en el mundo físico o digital, y no siempre con mayores garantías en este segundo caso (por ejemplo, el derecho al olvido: arts. 93 y 94). En otras ocasiones se regulan derechos, como el derecho a la desconexión, que ya derivan del derecho a la jornada laboral o el derecho al descanso y que sin embargo se condicionan ahora, parece, a la elaboración de una «política interna» por el empleador (art. 88.3). Se regulan de forma dispersa los derechos de los menores (arts. 84 y 92, pero también artículo 7 de la Ley). Se incorpora una controvertida regulación del llamado derecho al testamento digital (art. 96)[75], mientras que el artículo 3 se refiere a los datos de las personas fallecidas. Sin embargo se echa en falta alguna mención al derecho a la identidad en el entorno digital o el derecho de acceso al conocimiento. Todo ello sin perjuicio además de la necesidad de interpretar algunos preceptos de la Ley Orgánica que en su redacción final, no coherente con el texto final de la Ley Orgánica, deberían haberse retocado. Tal es el caso del artículo 47, que atribuye a la Agencia Española de Protección de Datos supervisar la aplicación de la entera Ley Orgánica, incluido por tanto el Titulo X en su totalidad.

En conclusión, la regulación de los derechos en la sociedad digital debe hacerse poniendo en el centro de la misma a la persona, partiendo de la base de que los derechos reconocidos en el entorno físico deben tener su reflejo en el entorno digital y con la perspectiva de normas que sean capaces de superar su obsolescencia a pesar de la innovación, para lo que es imprescindible volver a los principios y establecer un nuevo diálogo entre regulación y autorregulación.

74. Me remito en su totalidad al trabajo de Ignacio García-Perrote Escartín en esta misma obra.
75. Sobre ello, por todos, vid. Sergio Camara Lapuente, «La sucesión mortis causa en el patrimonio digital», *Anales de la Academia Matritense del Notariado*, 59, 2019, pp. 375 y ss.

4

PROTECCIÓN DE DATOS PERSONALES: RETOS PARA EL SISTEMA PENAL[1]

MERCEDES PÉREZ MANZANO
Catedrática de Derecho Penal, Universidad Autónoma de Madrid

4.1. INTRODUCCIÓN

La vertiginosa evolución tecnológica y la globalización han colocado a los datos personales en situación de permanente riesgo de ser conocidos, utilizados y difundidos por personas no autorizadas en cualquier lugar del planeta. A conjurar dichos peligros ha de contribuir, de forma esencial, el Derecho penal a través de la prevención y sanción de las conductas que afectan del modo más grave el *derecho a la autodeterminación informativa*, o derecho al control de la publicidad de los datos personales. El cumplimiento de dichas funciones de forma eficaz y legítima constituye un singular reto para el sistema penal, que debe enfrentar sin perder sus señas de identidad pero adaptándose a las características del actual modelo de sociedad en el que el uso de las tecnologías de la información y la comunicación (TIC) ha devenido imprescindible.

Como es sabido, el Derecho penal tiene, entre sus características legitimadoras, el constituir el último recurso al que el Estado debe acudir en la protección de los derechos de sus ciudadanos, porque esta rama del Derecho cuenta con medios de actuación especialmente drásticos y contundentes, singularmente restrictivos de los derechos de los ciudadanos. Por ello solo se debe acudir al Derecho penal cuando el resto de las instancias sociales y jurídicas se han mostrado insuficientes para la protección de la sociedad. En este marco, el primer reto al que se enfrenta el Derecho penal reside en fundamentar, de manera consistente, la específica necesidad de protección de los datos personales a través del Derecho penal partiendo de la trascendencia personal, social, política y económica que las TIC tienen en la sociedad actual. Pero, además, habrá de fundamentarse que la protección penal es congruente con el objeto y las necesidades de protección del mismo.

Pero no se trata solo de conseguir una apropiada y legítima protección penal de los derechos vinculados con el entorno digital cuando los particulares los vulneran, sino que se trata también de delimitar el marco en el cual el Estado puede reclamar

1. Este trabajo se corresponde, básicamente, con el texto de la conferencia que impartí en la Fundación Ramón Areces el 26 de junio de 2019. He mantenido, en lo sustancial, su estructura y contenido, añadiendo solo alguna cita bibliográfica.

de manera legítima el conocimiento y uso de datos personales de los ciudadanos, pues el cumplimiento de sus funciones lo requiere. Así sucede, sin duda, respecto de los órganos encargados de la persecución e investigación de los delitos, ya que el uso de las TICs constituye una herramienta indispensable para cumplir sus funciones. Los peligros para los datos personales no procederán entonces solo de los particulares, sino también del Estado, de las autoridades públicas que pueden verse tentados de sortear los mecanismos constitucionales de tutela de estos derechos en aras de conseguir objetivos, que mayoritariamente los ciudadanos consideramos legítimos. Sin duda la investigación de delitos es uno de esos objetivos legítimos, pero sin duda también, en el Estado de Derecho el fin no justifica cualquier medio para alcanzarlos por muy eficaz que este sea.

Pero antes de comenzar con la exposición, quiero realizar una precisión, que es paralelamente una declaración de principios. Forma parte del ADN del Derecho penal el constituir un instrumento de protección de la libertad y derechos de todos (los bienes jurídicos que se protegen) mediante la restricción de la propia libertad y derechos de los ciudadanos (al imponer sanciones que restringen los derechos de algunos y delimitar los ámbitos de actuación lícita). Esta característica del Derecho Penal es la razón que motiva a los penalistas a dedicar al menos el mismo tiempo a exponer por qué no se debe aplicar el Derecho penal que a justificar su utilización, y desde luego, explica que le dedicamos notables esfuerzos a argumentar la necesidad de limitar el uso del aparato penal por el Estado.

Esta manera de proceder de los penalistas suele resultar antipática para la mayoría de la ciudadanía porque cuando se habla de delitos y de Derecho penal, se piensa que los usuarios, los consumidores de ese Derecho penal, son otros, son los delincuentes a quienes se les ve como ajenos y distintos y, por tanto, como sujetos con menor legitimidad para invocar sus derechos fundamentales frente al Estado. Esta visión de la ciudadanía sobre la relación entre el Derecho penal y los derechos fundamentales no es acertada, pues olvida que un mayor uso y consumo de Derecho penal por el Estado no siempre conduce a mayores cotas de libertad o protección de los ciudadanos, sino que, en ocasiones acarrea una mayor restricción general de la libertad de todos, e incluso, un desbordamiento de los límites del Estado de Derecho vulnerando los derechos de algunos a quienes se convierte de forma ilegítima en delincuentes o delincuentes potenciales. Los peligros para la intimidad de los ciudadanos, para nuestro derecho a la libertad de autodeterminación informativa, proceden tanto de los particulares (al acceder, utilizar o difundir por razones privadas los datos personales de terceros), como del propio Estado (que también puede realizar intromisiones ilegítimas en los datos personales de los ciudadanos en el marco de una finalidad justificada, como es la investigación de la comisión de delitos)[2].

El enfoque dual de este trabajo tiene su anclaje en este rasgo del Derecho penal y en la necesidad de contrarrestar el equívoco señalado. Por ello, voy a referirme al modelo de protección de los datos personales en el Código penal a través de los delitos de descubrimiento y revelación de secretos, pero también al marco legíti-

2. Naturalmente también puede desbordar sus funciones aprovechando su capacidad de acceso a los datos personales. El caso más famoso en este ámbito es el conocido como caso de las *escuchas del CESID*, que dio lugar a la STS 22 de marzo de 2001, en la que se condenó a varios miembros de los servicios de inteligencia por vulnerar la intimidad de los ciudadanos mediante un sistema de escuchas telefónicas.

mo de restricción de los derechos a la intimidad, el secreto de las comunicaciones y la autodeterminación informativa en el contexto de la investigación delictiva. En lo que sigue, comenzaré por exponer brevemente cómo aparecen protegidos estos derechos en el Código penal, específicamente en el grupo de delitos denominados de descubrimiento y revelación de secretos; en segundo lugar, pondré de relieve algunos de los déficits de dicha regulación; y, finalmente, me ocuparé de exponer el marco en que puede ser legítima la restricción de dichos derechos en el contexto de la persecución e investigación delictiva a partir de la jurisprudencia interna e internacional.

4.2. LA PROTECCIÓN DE DATOS EN EL CÓDIGO PENAL ESPAÑOL

Los derechos relativos a los datos personales se protegen en el Código penal, principalmente, a través de un conjunto de figuras delictivas denominadas delitos de descubrimiento y revelación de secretos, que se encuentran recogidas en los artículos 197 y ss. CP. Pero no son estos los únicos delitos que se vinculan con los datos, pues el Código penal recoge otras figuras delictivas referidas a la protección de datos empresariales (art. 278 CP) e incorpora un conjunto de preceptos que involucran, de alguna manera, a los sistemas informáticos: así, la estafa informática (art. 248 CP), los delitos de daños informáticos (arts. 264, 264 bis, ter, quáter...), facilitar la comisión de los delitos contra la propiedad intelectual mediante sistemas informáticos (art. 270 CP), o falsear información relativa a la defensa nacional (art. 598 CP). De todos ellos solo me voy a referir a la protección de datos personales mediante los arts. 197 y ss., pues estos constituyen el núcleo esencial de protección penal de estos derechos.

4.2.1. Las modalidades delictivas

Una adecuada comprensión del sistema de protección penal de la intimidad y los datos personales configurado en el capítulo I (Descubrimiento y revelación de secretos) del Título X (Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio) del Código penal requiere tomar en consideración varios

elementos. De un lado, que el modelo se articula en torno a un conjunto de comportamientos que constituyen las modalidades básicas sobre las que pivotan una serie de agravaciones, lo que implica que solo podrán sancionarse como modalidades agravadas las conductas que reúnan los requisitos de la agravación además de los de la modalidad básica. De otro, hay que tener en cuenta que este capítulo es el fruto de una evolución legislativa, de modo que el resultado es un conjunto heterogéneo de figuras delictivas del que forman parte modalidades de corte tradicional así como nuevos tipos delictivos con una configuración más novedosa. Y, finalmente, que el eje central del sistema es la distinción entre las conductas de acceso a y apoderamiento de los datos, de un lado, y la revelación y difusión de los datos, de otro; conducta esta última que puede realizarse por quien previamente ha accedido de manera ilícita a los datos o por un tercero que no ha intervenido en la conducta previa.

El tipo básico de estos delitos que protegen la intimidad personal sanciona (con una pena de uno a cuatro años de prisión) al que, para descubrir los secretos o vulnerar la intimidad de otro, realice una de las tres conductas siguientes: a. se apodere de sus papeles, cartas, mensajes de correo electrónico, documentos o efectos personales; b. intercepte sus comunicaciones; c. o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o de cualquier otra señal de comunicación. Junto a la modalidad anterior, el Código Penal español siempre ha prestado una protección individualizada a los datos personales que figuran en registros sancionando con la misma pena a quienes sin estar autorizados se apoderan, alteran o utilizan en perjuicio de otro datos personales o familiares que se hallen registrados en ficheros o soportes informáticos, o en cualquier archivo público o privado. En este caso, se sanciona también a quien accede a dichos ficheros o registros sin estar autorizado. En tercer lugar, sanciona el Código penal las conductas de revelación, difusión o cesión de datos, hechos o imágenes a los que se refieren los delitos ya mencionados, imponiendo una mayor pena a quien difunde o revela los datos habiendo participado en el acceso a los mismos o en su apoderamiento, y sancionando con menor pena a quien solo los revela o difunde sin haber participado en la conducta previa de apoderamiento de los datos, pero conociendo su origen ilícito.

A partir de estas conductas se construyen una serie de modalidades agravadas. Así, se sanciona con mayor pena si quien realiza la conducta es la persona que tiene a su cargo el registro, si el sujeto activo es un funcionario público, si las conductas se realizan con la finalidad de obtener un beneficio económico o en el seno de una organización criminal o si los datos a los que afectan las conductas son los considerados «sensibles», es decir, aquellos datos que ofrecen información especialmente personal y cuyo conocimiento puede ser el presupuesto de un trato discriminatorio: ideología, religión, salud, origen racial, vida sexual, o referido a menores o persona con discapacidad necesitada de especial protección.

Junto a las conductas anteriores, en este marco más tradicional, el Código Penal contempla, de forma individualizada, el quebrantamiento del secreto laboral o profesional, es decir, la revelación de los secretos ajenos de los que se tenga conocimiento por razón de su oficio o relación laboral (art. 199.1) o el incumplimiento del deber de reserva o sigilo profesional divulgando los secretos de otro. Si el primero afecta a cualquier ciudadano en el seno de una relación laboral, el segundo solo afecta a quienes tienen legalmente establecido un deber de sigilo en el cumplimiento de su profesión, por ejemplo, abogados o médicos.

A los anteriores delitos se han incorporado nuevas modalidades delictivas. De un lado, se sanciona, si bien con una pena más leve (prisión de tres meses a un año)

la conducta consistente en revelar, difundir o ceder a terceros, sin autorización, imágenes o grabaciones audiovisuales que hayan sido obtenidas con consentimiento de su titular en lugar privado siempre que la divulgación menoscabe gravemente su intimidad personal (art. 197.7 CP). De otro, tras la incorporación de la responsabilidad penal de las personas jurídicas en 2010, los delitos de este capítulo pueden dar lugar a responsabilidad de las personas jurídicas si se dan los requisitos generales previstos en el art. 31 bis CP (art. 197 quinquies). Y, finalmente, esta regulación incluye el allanamiento informático (art. 197 bis CP) y sus actos preparatorios (art. 197 ter CP) que se sancionan con una pena de seis meses a dos años de prisión. Las conductas sancionadas en este delito son: el acceso, sin estar autorizado, a datos o programas de sistemas informáticos vulnerando las medidas de seguridad establecidas para impedir tal acceso; el mantenimiento en el sistema informático sin autorización del titular, aunque haya accedido a él de forma legítima; la interceptación de transmisiones no públicas de datos informáticos, sin estar autorizado, realizadas mediante la utilización de artificios o instrumentos técnicos, incluidas las emisiones electromagnéticas de los mismos; y, por último, la producción, adquisición para su uso, importación o facilitación a terceros de cualquier modo de un programa informático –concebido o adaptado principalmente para cometer dichos delitos–, o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información, sin estar debidamente autorizado y con la intención de facilitar a terceros la comisión de estos delitos.

4.2.2. Retos para una adecuada configuración legal e interpretación judicial

Como acabo de referir, en esta regulación conviven los delitos tradicionales de descubrimiento y revelación de secretos junto al más moderno allanamiento informático y esta cohabitación, el compartir título y capítulo del Código penal, no es fácil porque da pie a intentar realizar una interpretación unitaria de todas las figuras delictivas, de reconducirlas a bienes jurídicos comunes, lo que puede tener efectos contraproducentes para una adecuada protección penal de todo el universo de conductas que pueden afectar a los datos personales y/o a la intimidad. Desde esta perspectiva, el primer reto al que me voy a referir es el de una correcta definición de los bienes jurídicos y derechos protegidos. En segundo lugar, me ocuparé de la necesidad de mejora técnica de algunos tipos penales. Ahora bien, como decía al comienzo, en el Estado de Derecho, el fin no justifica los medios, de modo que el segundo desafío, al que se enfrentan tanto el legislador penal como los jueces reside en la configuración y aplicación de los delitos sin conculcar los principios y garantías penales. Esta será entonces la tercera cuestión que trataré en este epígrafe.

¿Unidad o pluralidad de bienes jurídicos protegidos?

La primera reflexión a realizar para saber si la regulación penal es adecuada se refiere a cuál o cuáles son los bienes o derechos protegidos en estas modalidades delictivas y, de forma singular, si en las modalidades tradicionales se protegen los mismos derechos que en las figuras más modernas como el denominado intrusismo o allanamiento informático. La respuesta reside en que aunque todos tienen un tronco común que es la intimidad, sin embargo, todas modalidades delictivas no protegen sólo ni de la misma manera este bien jurídico protegido.

En efecto, si bien no cabe duda de que las modalidades tradicionales protegen la intimidad personal, sin embargo, el allanamiento informático no exige la vulne-

ración de dicho derecho aunque tenga o pueda tener en muchos casos una conexión con la intimidad personal. En realidad, como ha sido puesto de relieve por la doctrina[3], estos novedosos delitos protegen no sólo la privacidad informática, sino también su seguridad, es decir, la libertad de uso, confidencialidad e integridad de los sistemas informáticos y los datos de todo tipo que contienen. De conformidad con la regulación europea, el Código penal ha establecido una regulación diferenciada respecto a los delitos tradicionales, en el entendimiento de que no es lo mismo el acceso o revelación de datos de carácter personal que el acceso a datos del software empleado o de la situación de los puertos de entrada y salida de un sistema informático. Por ello también se distingue entre la interceptación de transmisiones de datos personales y la interceptación de las transmisiones automatizadas entre equipos informáticos. El allanamiento o intrusismo informático sanciona el acceso a sistemas informáticos con independencia de su vinculación con el derecho a la intimidad personal. Su finalidad es proteger el derecho al control de la publicidad de cualesquiera tipo de datos, pero también proteger los sistemas informáticos en sí mismos frente a las interferencias en el sistema. La razón que avala esta singular protección es clara: es necesario que el uso de los sistemas informáticos pueda realizarse en condiciones de libertad (poder de disposición) y seguridad, de tal modo que se garantice su integridad y la propia reserva o confidencialidad del sistema.

Es cierto que protegiendo los sistemas informáticos se protege también la intimidad personal, pero también lo es que no sólo se protege esta, puesto que también se garantizan otros intereses de particulares, empresas o Administración pública:

3. Por ejemplo, Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, Derecho penal e internet, en Cremades, Fernández-Ordóñez, Illescas (ed.), Régimen jurídico de internet, La Ley, Madrid, 2002, pp. 260-262, 269; Carrasco, M., en Álvarez, J. (dir.), Derecho penal español, Parte Especial, (I), 2ª ed., Tirant lo blanc, Valencia, 2011, p. 783; Rueda, M. A., La nueva protección de la vida privada y de los sistemas de información en el Código penal, Atelier, Barcelona, 2018, pp. 52 y ss. Sobre la polémica en torno al bien jurídico protegido, cfr. Rueda, M. A., La nueva protección de la vida privada y de los sistemas de información en el Código penal, pp. 47 y ss.

intereses económicos (patrimoniales, la propiedad intelectual e industrial), la seguridad nacional, el buen funcionamiento de las infraestructuras o de los sistemas críticos, la capacidad competitiva de las empresas, la Administración electrónica, el comercio electrónico, la domótica o gestión doméstica a distancia, o el sistema sanitario... Protegemos los sistemas informáticos porque es una forma de proteger todos esos bienes jurídicos mediatos frente a los peligros que derivan del uso de la informática. En la Sociedad de la Información, la integridad, confidencialidad, autenticidad (fiabilidad) y disponibilidad de los datos y de los sistemas informáticos[4] son valores esenciales para garantizar el modelo actual de relaciones sociales, económicas y políticas. Como afirmaron hace ya tiempo Rodríguez Mourullo, Lascuraín y Alonso[5], los bienes protegidos bajo la denominación genérica de privacidad informática, son bienes instrumentales de la protección de otros bienes e intereses involucrados con el uso de los sistemas informáticos, de modo que la protección de los sistemas informáticos actúa como barrera de contención de riesgos para esos otros bienes. Es la importante función social de los sistemas informáticos la que dota de legitimidad la protección penal autónoma de este bien jurídico: la integridad, confidencialidad, autenticidad (fiabilidad) y la disponibilidad de los datos y de los sistemas informáticos.

La configuración del bien jurídico protegido en este delito como un derecho autónomo, es fundamental para su interpretación y aplicación, pues dicha autonomía e independencia implica que no sea necesario ni que se vinculen a privacidad personal alguna (ni siquiera exigiendo el peligro para dicho bien jurídico), ni que se exija en el caso concreto que el acceso al sistema informático o la interceptación de la transmisión se haya producido con la intención de desvelar la intimidad de otro[6] que es requisito de las modalidades clásicas y cuya exigencia dejaría significativas lagunas de protección penal[7].

A mi modo de ver, algunas de las ácidas críticas de la doctrina penalista esgrimidas contra la regulación penal responden a una falta de comprensión correcta de la importancia que estos bienes jurídicos tienen por sí mismos y en relación con aspectos esenciales de nuestro modelo social. Se ha criticado mucho, en la doctrina,

---

4. La integridad del sistema informático alude a que no se modifique el contenido de la información contenido en el sistema; la confidencialidad, a que solo va a ser utilizado por las personas autorizadas; la disponibilidad se refiere al control sobre la utilización del sistema. Estos tres valores pueden verse afectados por el mero acceso a un sistema informático sin autorización, es decir, por el denominado hacking blanco, que no tiene pretensiones de dañar el sistema, de vender los datos, etc. *Sobre la fenomenología criminal*, cfr. Miró, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, passin; sobre el hacking blanco, pp. 53 y ss.
5. Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, *Derecho penal e internet*, p. 261.
6. A favor de la interpretación de estos delitos en conexión con el bien jurídico intimidad, considerando que se trata de un delito de peligro abstracto, por todos Anarte, E./Doval, A., «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio» (1). «Descubrimiento y revelación de secretos», en Boix, J. (dir.), *Derecho Penal, Parte Especial*, vol. I, 2ª ed., Madrid, Iustel, 2016, pp. 493 y ss., 517; Bolea, C., en Corcoy (dir.), *Manual de Derecho Penal. Parte Especial*. Tomo I., 2ª ed.Tirant lo Blanc, Valencia, 2019, pp. 340 y ss.
7. Un sector doctrinal interpreta que el bien jurídico, seguridad informática, sólo se protege en relación con las infraestructuras críticas, por entender que ello deriva del principio de proporcionalidad. Cfr. Castiñeira/Estrada, en Silva Sánchez (dir.), *Lecciones de Derecho penal. Parte Especial*, Atelier, 4ª ed., Barcelona, 2015, p. 164.

el allanamiento informático[8] porque la conducta no requiere vinculación con el bien jurídico intimidad personal. Se afirma que esta disposición es consecuencia de la imparable –inútil y contraproducente– «escalada del Derecho penal hacia el "riesgo cero"»[9], es decir, hacia la punición de cualquier riesgo. Pero por las razones expuestas, relativas a las esenciales funciones que desempeñan los sistemas informáticos en la sociedad actual, entiendo que es legítima la intervención penal en este ámbito: la confidencialidad, la integridad y la disponibilidad de los sistemas de información constituyen una barrera de contención de riesgos para otros bienes jurídicos que se pueden ver involucrados en la función social de los sistemas informáticos (el patrimonio, la intimidad...).

No obstante, también se debe ser consciente de que el delito de allanamiento informático se sanciona con una pena menos grave que la que acarrean los delitos tradicionales contra la intimidad y ello se debe a que el allanamiento informático implica una anticipación de la tutela y de la punición de otras conductas[10] que se encuentran más próximas a la lesión de los bienes jurídicos mediatos que se quieren proteger. Por consiguiente, si mediante el acceso a un sistema informático se vulnerase la intimidad personal, ya no se aplicaría el delito de intrusismo informático sino el de descubrimiento y revelación de secretos tradicional, pues el desvalor de aquel quedaría absorbido por el de este[11].

En suma, la respuesta a la pregunta que nos hacíamos es que la regulación penal protege una pluralidad de bienes jurídicos estrechamente conectados, de tal manera que la conexión existente entre ellos debe presidir la interpretación de los tipos delictivos y las soluciones sobre los eventuales concursos entre ellos.

¿Están configurados los tipos penales de forma técnicamente correcta?

Si bien constituye siempre un reto para el legislador penal formular los tipos de forma correcta, en este ámbito el reto es mayor pues también es mayor la complejidad de la materia regulada. Quizás por ello, restan algunos déficits que deberían intentar corregirse.

Un primer problema que se plantea es de orden sistemático, pues, como ya he mencionado, no parece adecuado que el intrusismo o hacking informático se haya incorporado al grupo de los delitos contra la intimidad cuando además de los bienes jurídicos inmediatos a los que me he referido, se protegen otros valores que carecen de conexión con la intimidad personal[12]. De hecho, esta ubicación permite ciertas

8. Anarte, E./Doval «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos», en Boix, J. (dir.), *Derecho Penal, Parte Especial*, vol. I, pp. 493 y ss., 512, 517-520.
9. Anarte, E./Doval, «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos», en Boix, J. (dir.), *Derecho Penal, Parte Especial*, vol. I, 1ª ed., 2010, p. 455.
10. Sobre ello, Miró, F., «Delitos informáticos. Hacking. Daños». En Ortiz de Urbina (coor.), *Memento Experto. Reforma penal 2010*. Ley Orgánica 5/2010, Ediciones Francis Lefebvre, Madrid, 2010, Nº marginal 1438.
11. Por todos Anarte, E./Doval, A., «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos», en Boix, J. (dir.), *Derecho Penal, Parte Especial*, vol. I, p. 511; Guérez, P., «Descubrimiento y revelación de secretos», en Molina, F. (dir.), *Memento práctico penal*, Ed. Francis Lefebvre, 2019, nº marginal 9941.
12. Por su ubicación en un título independiente como delitos contra los sistemas informáticos se

interpretaciones de esta modalidad delictiva[13] que, al vincularla con la intimidad personal, exigen el peligro para esta[14], lo que restringiría el campo de aplicación del intrusismo informático hasta excluirlo en los casos mencionados de acceso a sistemas informáticos, como las infraestructuras críticas, que carecen de conexión con la intimidad personal. Sin perjuicio de que la salida de este delito de los apartados del artículo 197 para integrar otro delito posterior, el 197 bis, parece ir en la dirección apuntada de individualizar esta modalidad delictiva, mientras se mantenga en el título X del Código penal será difícil no efectuar dichas interpretaciones.

En segundo lugar, se constatan solapamientos entre las distintas figuras delictivas, lo que genera problemas de interpretación y problemas concursales. En este contexto sería necesaria una delimitación más precisa entre las modalidades delictivas tradicionales y el nuevo delito del art. 197 bis. Por ejemplo, en relación con el acceso y utilización de datos de un registro, a pesar de diferencias en la literalidad de los preceptos, lo cierto es que quien accede a un registro de datos que figura en un sistema informático y altera los datos en perjuicio de alguien, también está paralelamente accediendo a un sistema vulnerando las medidas de seguridad, por tanto realiza a la vez las dos conductas. Es decir, estamos ante un concurso, que en caso de ser de normas se resuelve con la aplicación de un solo delito y la pena que le corresponda, mientras que si es de delitos, será posible agravar la pena e incluso

---

ha manifestado la doctrina, por ej., Guérez, P., «Descubrimiento y revelación de secretos, en Molina», F. (dir.), *Memento práctico penal*, nº marginal 9947.

13. A favor de la salida del allanamiento informático del art. 197 se ha manifestado, Zárate, A., «La tutela penal de los datos de carácter personal. Una perspectiva jurisprudencial». *Diario La Ley*, nº 9422, mayo, 2019, p. 3.
14. Por todos Anarte, E./Doval, Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Descubrimiento y revelación de secretos, en Boix, J. (dir.), *Derecho Penal, Parte Especial*, vol. I, p. 517. A favor de una interpretación restrictiva del allanamiento informático también, Guérez, P., Descubrimiento y revelación de secretos, en Molina, F. (dir.), *Memento práctico penal*, nº marginal 9949; Tomás-Valiente Lanuza, C., Capítulo I. Descubrimiento y revelación de secretos, en Gómez Tomillo, M., Comentarios prácticos al Código penal, Tomo II, Cizur Menor, Aranzadi, pp. 653 y ss., 675; La misma, Delitos contra la intimidad y redes sociales (en especial en la jurisprudencia más reciente), en IDP, Revista de Internet, *Derecho y Política*, nº 27, 2018, p. 38.

sumar las penas por los varios delitos cometidos. La solución de esta relación concursal depende de la interpretación que demos a los bienes jurídicos protegidos y a la conexión típica entre las conductas. A mi modo de ver, se trata de un concurso de normas[15], pues la confidencialidad del sistema informático, que es el valor protegido, es instrumental respecto de la protección de la intimidad personal y casi una parte del mismo, de modo que el acceso al sistema informático no es sino un estadio previo necesario para conseguir la utilización de los datos del registro. Por consiguiente, solo aplicaríamos el art. 197.2 CP y la pena en él prevista –prisión de uno a cuatro años–.

Pero no solo hay solapamientos entre los tipos, sino también algunas lagunas, es decir, casos cuya calificación típica y sanción en el marco de estos delitos resulta harto discutible, cuando no prohibida por constituir una interpretación analógica lesiva del principio de legalidad, a pesar de que existen razones para entender que no era intención del legislador dejar fuera del Código penal dichas conductas y a pesar de existir consenso sobre su necesaria sanción penal. Así sucede con la conducta consistente en difundir sin su consentimiento lo que la propia víctima ha grabado o fotografiado y enviado a un tercero, que no encaja en el art. 197.7 CP introducido en la reforma operada en la LO 1/2015. Literalmente, este precepto requiere que las imágenes se hayan obtenido o grabado por el tercero con la anuencia de la víctima, por lo que si han sido grabadas por la propia víctima la conducta es atípica. A pesar de ello, la interpretación mayoritaria de doctrina y jurisprudencia[16] incluye este supuesto en el ámbito del tipo, lo que es muy discutible desde la óptica de la prohibición de la analogía *in malam partem* que rige en el Derecho penal[17].

¿Respeta la regulación penal los principios y garantías penales?

El tercero de los desafíos a los que se enfrenta el legislador penal reside en configurar una legislación respetuosa con los principios penales que son manifestación del Estado de Derecho en este ámbito. Uno de estos es el principio de proporcionalidad de las penas, concreción del principio de igualdad ante la ley y del valor justicia. Conforme a este principio, las penas deben reflejar la distinta gravedad de las conductas, de modo que las mismas magnitudes de penas deben sancionar delitos de una gravedad similar. Pues bien, la regulación de estos delitos no respeta este principio, pues se sancionan con las mismas penas conductas cuya gravedad no es similar.

En primer lugar, merece crítica la equiparación de penas entre conductas de autoría y de complicidad que se establece en este capítulo del Código penal[18], como por

15. En el mismo sentido, cfr. Tomás-Valiente Lanuza, C. (Delitos contra la intimidad y redes sociales (en especial en la jurisprudencia más reciente), en IDP, Revista de Internet, *Derecho y Política*, nº 27, 2018, pp. 30 y ss., 38, 39. Esta autora se manifiesta a favor de considerar concurso de leyes a resolver por el principio de consunción en favor de los arts. 197.1 o 2 en los casos de entrada no autorizada, venciendo las barreras de protección, al correo electrónico de otra persona o un registro de un banco, Seguridad Social, etc., pero se utiliza para acceder a material íntimo. Igual tratamiento le merecen los casos de acceso a los mensajes particulares dentro de las redes sociales, realizado por quien se ha introducido en la página privada de alguien.
16. Cfr. SAP Sevilla 314/2017, de 28 de junio; SSAP Valencia 488/2016, de 25 de noviembre, y 528/2017, de 7 de septiembre. En la doctrina, por todos, Morales, F., Comentarios al art. 197 CP, en Quintero, G./Morales, F., Comentarios al Código penal de 1995, tomo I, 7ª ed., Cizur Menor, Aranzadi, 2016, pp. 1434 y ss., 1466-73.
17. Cfr. Tomás-Valiente Lanuza, C. Delitos contra la intimidad en IDP nº 27, 2018, p. 34.
18. En este sentido por todos Rueda, M. A., La nueva protección de la vida privada y de los sistemas

ejemplo, la equiparación entre el acceso al sistema informático y facilitar el acceso a otro, pues en sentido dogmático-penal la conducta consistente en facilitar el acceso es una conducta constitutiva de colaboración o participación en el hecho principal que otro realiza (el acceso al sistema informático) que calificaríamos como complicidad o en su caso cooperación necesaria, de modo que conforme a las reglas generales, no siempre debería sancionarse con la misma pena que el autor del delito. Y, en segundo lugar, también constituye una desproporción sancionar con la misma pena los actos preparatorios y los actos de ejecución delictiva. Así, las penas previstas para el acceso al sistema informático son las mismas previstas para la creación de los programas informáticos con la intención de facilitar la comisión de estos delitos, a pesar de que esta última conducta constituye un mero acto preparatorio de la primera, alejado aún de la eventual vulneración de la intimidad personal o de la confidencialidad del sistema informático. Con esta expresa tipificación de actos preparatorios no solo se produce una anticipación excesiva de la tutela penal y su sanción de forma desproporcionada[19], sino también una configuración delictiva que va a plantear muchos problemas de delimitación respecto de conductas lícitas y sobre todo de prueba de alguno de los elementos típicos. Así, la creación de programas generadores de claves puede tener como finalidad la recuperación de las mismas por los propios usuarios cuando las han perdido o se han bloqueado, de manera que no resulta fácil establecer criterios para determinar cuándo la posesión de dichos programas obedece a la intención de facilitar estos programas a otros para cometer el delito de allanamiento informático. Y estas dificultades prácticas, de delimitación y prueba de las conductas delictivas, pueden conducir en muchas ocasiones a una relajación de las exigencias del derecho a la presunción de inocencia, derecho, que también se proyecta sobre la prueba de los elementos subjetivos de los delitos.

Como conclusión de esta primera parte se puede afirmar que, si bien la legislación penal está en la línea adecuada para proteger correctamente los datos personales en el entorno digital, dado que se han conseguido identificar bienes jurídicos autónomos en el contexto de lo que la legislación europea estaba demandando, deslindándose las conductas que afectan a la intimidad de las que menoscaban la seguridad de los sistemas informáticos, sin embargo, esta regulación presenta algunos déficits tanto de carácter técnico como político-criminal que requieren todavía de una reflexión sosegada y alguna modificación legislativa.

4.3. LA INVESTIGACIÓN JUDICIAL DE LOS DELITOS Y LA PROTECCIÓN DE LOS DATOS PERSONALES

4.3.1. Las garantías constitucionales anudadas a las limitaciones de los derechos reconocidos en el art. 18 CE

La jurisprudencia clásica sobre la protección constitucional diferenciada de los derechos a la intimidad y al secreto de las comunicaciones

La investigación judicial de delitos está presidida por el contenido del art. 18 de la

de información en el Código penal, p. 191.

19. En este sentido por todos Morales Prats, F., Comentarios al art. 197, en Quintero/Morales (dir.), Comentarios al Código Penal Español, Tomo I, p. 1485.

CE[20], que, en lo que nos interesa, establece, de un lado, la necesidad de recurrir a la autorización judicial para la interceptación de las comunicaciones y el registro domiciliario (números 2º y 3º del art. 18 de la CE) y un régimen menos estricto de limitación o restricción del derecho a la intimidad personal o la protección de datos (números 1º y 4º del art. 18 del CP) para los que no se exige siempre dicha autorización. Requisitos comunes para afirmar la legitimidad de la restricción todos los derechos son: que esta obedezca a una finalidad legítima, que la restricción se encuentre habilitada en una norma de rango legal y que tal limitación sea necesaria y proporcionada –por todas STC 70/2002, de 3 de abril–. El Tribunal Constitucional ha admitido que en los casos en que tan sólo esté en juego el derecho a la intimidad se pueda prescindir excepcionalmente de la resolución judicial motivada que autorice la injerencia, así, por ejemplo, en los casos de necesidad de una intervención policial inmediata (STC 70/2002).

Este diferente tratamiento jurídico-constitucional de los derechos del art. 18 de la CE implica que la interceptación de una comunicación telefónica mientras está teniendo lugar para grabar las comunicaciones está sometida al requisito de la previa autorización judicial, mientras que si se accede a una agenda privada que uno guarda en el bolsillo, no sería siempre necesaria la autorización judicial. Si en el primer caso estamos ante el núcleo protegido por el art. 18.3 de la CE (secreto de las comunicaciones), en el segundo caso estamos ante el contenido garantizado por el art. 18.1 de la CE (la intimidad personal). Esta diferenciación tiene su origen en la jurisprudencia constitucional elaborada desde comienzos de los años ochenta del pasado siglo en un intento de configurar un ámbito propio para cada uno de los preceptos o párrafos del art. 18 de la CE, puesto que su tenor literal es distinto. Es además, en ese marco de interpretación del art. 18 de la CE, en este caso de su párrafo cuarto, en el que el Tribunal Constitucional ha desarrollado el derecho a la protección de datos a partir de un tenor literal poco adecuado al efecto, pues este precepto tan sólo establece que «[l]a 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».

Las insuficiencias de la jurisprudencia constitucional clásica para la protección de los datos personales en el marco de la investigación judicial

A nadie se le oculta que este marco normativo constitucional no es el más idóneo para la protección de los datos personales en el entorno digital, pues estas diferenciaciones carecen de sentido ya que conducen, por ejemplo, a sostener que el correo electrónico una vez descargado y depositado en la bandeja de entrada quedaría protegido por el derecho a la intimidad personal y no por el derecho al secreto de las comunicaciones, por lo que el acceso al mismo no siempre requerirá autorización judicial.

La razón que sustenta, de conformidad con la jurisprudencia constitucional, este diferente régimen jurídico reside en el mayor riesgo de vulneración del derecho

20. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. 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.

al secreto de las comunicaciones –frente al derecho a la intimidad personal– que procedería de los propios mecanismos técnicos a través de los cuales se accede a las comunicaciones. Pues bien, parece bastante evidente que el desarrollo de las TIC en la actualidad ha colocado tanto a la intimidad como al secreto de las comunicaciones en la misma situación de exposición a los riesgos de injerencia ilegítima, sin que sea posible efectuar diferenciaciones, porque los peligros proceden del uso de las tecnologías y de que estas permiten el acceso remoto y masivo al ordenador, a todas sus funciones. Desde esta perspectiva, deberíamos repensar si lo más peligroso o lo que más afecta nuestra privacidad es la interceptación en tiempo real de la comunicación. Una reflexión sobre las funciones, contenido y acceso a las distintas partes de un ordenador puede servirnos de ejemplo: conforme a la diferenciación tradicional, si se accede a las fotos o a la agenda se estaría afectando la intimidad personal, mientras que si se intercepta el envío de un correo electrónico estaríamos ante una injerencia en el secreto de las comunicaciones que requiere siempre autorización judicial. ¿Es realmente adecuado este régimen dual de acceso legítimo a los dispositivos electrónicos dependiendo de la parte o función del mismo que resulte afectada?

El modelo unitario de tratamiento jurídico de las injerencias en los datos personales

El Tribunal Supremo ha sido consciente de que el diferente régimen de legitimidad de las injerencias en estos derechos no constituye un marco adecuado para la protección de los datos personales en el entorno digital y ha comenzado a unificar el régimen de garantías necesarias para que la limitación o restricción de este/os derecho/s sea legítima.

Así, en relación con los ordenadores, la STS 342/2013, de 17 de abril (FJ 8), sostiene que:

> «[e]l acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos

de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE (RCL 1978, 2836)). Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. .../... En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. ... / La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, ... toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. .../... Sea como fuere, ... la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías».

En suma, con toda la razón, el Tribunal Supremo ha decidido unificar los requisitos de la legitimidad del acceso a un ordenador dado que este puede albergar una multiplicidad de información de distinto carácter y dado que, por tanto, su acceso puede afectar tanto a la intimidad personal como al secreto de las comunicaciones. Y esta unificación se ha hecho al alza, exigiendo siempre una autorización judicial previa para acceder al contenido del ordenador. De otra parte, como ha quedado expuesto, el Tribunal Supremo exige que dicha autorización judicial sea individualizada, no siendo suficiente la autorización judicial que permite la entrada y registro del domicilio en el que puede encontrarse el ordenador: es necesario que el juez pondere específicamente la proporcionalidad del sacrificio de los derechos vinculados con el

entorno digital, «aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías»[21].

Esta misma protección unificada ha sido trasladada al teléfono móvil. Así, la STS 204/2016, de 10 de marzo afirma expresamente que la consideración diferenciada de cada uno de los derechos afectados de forma separada es insuficiente para garantizar una protección eficaz, pues resulta difícil garantizar que una vez permitido el acceso directo a datos protegidos por el derecho a la intimidad no se acceda a otros datos tutelados por el secreto de las comunicaciones. Por ello se afirma que debe darse una protección unitaria a estos dispositivos electrónicos al amparo de un «derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual».

Algunas insuficiencias de la jurisprudencia constitucional actual

El Tribunal Constitucional ha sido consciente también de los problemas que su jurisprudencia podría acarrear en relación con el acceso al teléfono móvil. En la STC 230/2007, de 5 de noviembre, declaró la vulneración del secreto de las comunicaciones del art.18.3 de la CE en un caso en el que la policía había accedido al registro de llamadas que había quedado en el móvil al incautárselo a su titular sin solicitar autorización judicial. Sin embargo, otras resoluciones evidencian que no ha realizado una reflexión global de la necesidad de unificación del tratamiento de la intimidad informática con el secreto de las comunicaciones. De hecho, el caso examinado en una de las Sentencias del Tribunal Constitucional más citadas en este tema, la STC 173/2011 de 7 de noviembre, ha dado lugar a una condena a España por el Tribunal Europeo de Derechos Humanos en una sentencia de 2017.

El caso de la STC 173/2011 puede ser ilustrativo de varios de los problemas que se suscitan en este tema: de un lado, las disfunciones de la existencia de un

21. En el mismo sentido SSTS 786/2015, de 4 de diciembre, 204/2016, de 10 de marzo, 287/2017, de 19 de abril.

canon diferenciado; de otro, los desajustes ocasionados por la existencia de diferentes estándares de protección de estos derechos a nivel interno e internacional. Como vamos a ver, la STEDH, de 30 de mayo de 2017, declaró que se había producido la vulneración del art. 8 del CEDH mientras que el Tribunal Constitucional español había denegado previamente el amparo por vulneración del derecho a la intimidad del art. 18.1 de la CE. Los hechos del caso analizado, sucintamente expuestos, son los siguientes. Un sujeto llevó el ordenador al técnico informático para que le reparase la grabadora que no funcionaba. El técnico, tras efectuar las reparaciones necesarias, eligió al azar algunos archivos del disco duro para grabarlos y comprobar si la grabadora funcionaba. En este proceso se encontró con archivos, vídeos y fotografías, que tenían contenido delictivo, por lo que denunció a la policía los hechos. La policía intervino el ordenador y procedió a su registro y análisis sin solicitar autorización judicial. Para argumentar la legitimidad de su actuación, la policía sostuvo, de un lado, que cuando el técnico le pidió la contraseña al titular del ordenador para acceder al mismo, este contestó que el aparato carecía de contraseña y, de otro lado, que su dueño tenía configurado el ordenador de modo que el programa de descarga de archivos permitía que cualquiera accediera a su ordenador para compartir los archivos. Es decir, la policía adujo que existía un consentimiento genérico del titular del ordenador que autorizaba el acceso al mismo.

En su análisis del caso, el Tribunal Constitucional comenzó afirmando que el técnico que reparó el ordenador no se había extralimitado en el uso del mismo, pues se había limitado a acceder a los archivos para comprobar la reparación de la grabadora, cosa que su titular sabía y para lo que había sido autorizado. Por ello el Tribunal Constitucional razonó que, siendo el hallazgo casual y teniendo todo ciudadano obligación de denunciar la comisión de delitos, el técnico estaba obligado a denunciar los hechos ante la policía (FJ 5). Ahora bien, cuando la policía accedió al ordenador no solo entró en los documentos del mismo sino en la carpeta *Incoming* del programa de descarga Emule. Por dicha razón, el Tribunal Constitucional afirmó que la autorización dada por el propietario del ordenador no alcanzaba esta clase de actuación de la policía y que ni siquiera se podría admitir la existencia de una autorización genérica, pues la autorización dada al técnico no abarcaba esa clase de uso del ordenador, el realizado por la policía.

El Tribunal Constitucional no detuvo ahí su análisis del caso, sino que examinó si un acceso sin consentimiento de su titular podía ser constitucionalmente legítimo llegando a afirmar que el acceso realizado en el caso lo era: primero afirmó que la actuación obedecía a una finalidad legítima, la investigación de delitos; en segundo lugar, sostuvo que la injerencia estaba prevista en la ley; y, en tercer lugar, razonó que la injerencia había sido necesaria y proporcionada. En particular, el Tribunal Constitucional apeló a la necesaria celeridad de la actuación policial en el caso, a la dificultad de persecución de este tipo de delitos por utilizarse las TICs, a la necesidad de que la policía asegure las pruebas incriminatorias, y a la propia gravedad de los delitos investigados. Además, añadió que la ejecución del registro del ordenador fue proporcionada, y que a los dos días se puso el mismo en conocimiento del juzgado de instrucción. En suma, el modelo de razonamiento del Tribunal Constitucional en este caso, esto es el test de legitimidad aplicado, se ajusta al del derecho a la intimidad personal del art. 18.1 de la CE, conforme al cual no es siempre necesaria la autorización judicial previa, pero sí que materialmente se ajusta a las exigencias del principio de proporcionalidad.

La resolución de este caso no suscitó la unanimidad del tribunal, pues la sentencia cuenta con un voto particular discrepante de la magistrada Elisa Pérez Vera. La argumentación del mismo se articula en torno a dos ideas: la falta de calidad de la ley habilitadora de la restricción del derecho fundamental y la falta de proporcionalidad de la propia limitación del derecho. En concreto, en relación con este último aspecto, el voto particular razona que no era necesario ni urgente el registro del ordenador por la policía ya que el dueño estaba detenido y la policía tenía el ordenador en su poder, por tanto, los riesgos a los que se alude en la sentencia eran inexistentes: estando detenido su propietario, el acceso y registro del ordenador por parte de la policía podía esperar a que se tramitara la autorización judicial.

La STEDH de 30 de mayo de 2017, asunto Trabajo Rueda c. España, dio parcialmente la razón al voto particular al sostener que el registro del ordenador en las condiciones en que se efectuó no fue proporcionado a pesar de que la limitación del derecho a la protección de los datos contenidos en el ordenador tenía una finalidad legítima.

> «En opinión del Tribunal, en este caso, es difícil valorar la urgencia que habría obligado a la policía a registrar los archivos del ordenador personal del demandante y acceder al contenido, sin obtener previamente la autorización judicial normalmente requerida. En efecto, no existía ningún riesgo de desaparición de ficheros puesto que el ordenador lo tenía la policía y no estaba conectado a Internet. El Tribunal no consigue descubrir las razones por las que la espera de una autorización judicial previa a la intervención sobre el ordenador del demandante, que podía haber sido obtenida rápidamente, habría dificultado la investigación sobre los hechos denunciados llevada a cabo por la policía» (pár. 46).

Como vemos, tampoco la jurisprudencia del Tribunal Europeo de Derechos Humanos requiere siempre la autorización judicial previa para afirmar la legitimidad de la restricción del derecho a la intimidad establecido en el art. 8 del CEDH. Ello se debe a que el Tribunal Europeo tiene que coordinar los modelos de protección de los derechos fundamentales de todos los países europeos y en algunos de ellos la función de control de la legitimidad constitucional de las intervenciones de las comunicaciones no la ejerce el órgano judicial sino la fiscalía (por ejemplo en Alemania). Por dicha razón, al Tribunal Europeo de Derechos Humanos le importa más el análisis sustantivo de la proporcionalidad estricta de la limitación del derecho, dando por válido que en algún caso puede estar justificada la ausencia de un control del sacrificio del derecho por parte de un órgano ajeno al poder ejecutivo y las fuerzas de seguridad del estado.

En cualquier caso, aunque el Tribunal Europeo de Derechos Humanos admita la legitimidad de limitaciones del derecho a la intimidad no autorizadas judicialmente, ello no debe conducirnos a sostener que dicha posibilidad es válida a nivel interno, pues el estándar de los derechos reconocidos en el Convenio Europeo de Derechos Humanos tiene la condición de mínimos, siendo nuestra constitución más garantista. Por ello entiendo que se ha de seguir la línea garantista y unificadora iniciada por el Tribunal Supremo que exige siempre autorización judicial individualizada para limitar los derechos vinculados con el entorno digital.

4.3.2. Las limitaciones a la protección de los datos personales por razón de la investigación judicial en el Derecho Europeo

El Reglamento 2016/679 y la Directiva 2016/680 del Parlamento y del Consejo de 27 de abril de 2016[22]

Como es sabido, el Reglamento y la Directiva, de idéntica fecha, regulan los derechos relativos a la protección de datos de las personas físicas en el ámbito de la Unión Europea, refiriéndose la Directiva específicamente a las garantías necesarias para la protección de datos personales cuando se utilizan en la investigación penal y cuando se transmiten internacionalmente como fruto de la cooperación judicial internacional en el ámbito de la Unión Europea. Objetivo expreso de esta directiva (art. 2) no es solo la protección de datos personales sino garantizar su intercambio en el ámbito de la Unión Europea[23] porque dicho intercambio constituye un mecanismo necesario para la mayor efectividad de la persecución de los delitos. En ese doble objetivo, reside, quizás, la causa de los problemas de esta regulación, pues la lógica de la protección de los derechos fundamentales es muy distinta y, en muchas ocasiones, opuesta a la lógica de la libre circulación de datos y a la de las necesidades de eficacia en la lucha contra la criminalidad.

Ambas normas prevén la posibilidad de limitar la protección de los derechos relativos a los datos personales. En sí misma, esta previsión no merece crítica, pues cualquier derecho fundamental puede estar sujeto a limitaciones legítimas. Ahora bien, lo que llama la atención de esta regulación es tanto el carácter amplio de la previsión, como sobre todo su propia vaguedad.

Así, con carácter general, el art. 23 del Reglamento se refiere a la posibilidad de que mediante legislación europea o nacional se establezcan limitaciones del «alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22». Y para que dichas previsiones sean legítimas requiere que se respete el contenido esencial de estos derechos y libertades y que las medidas establecidas sean necesarias y proporcionadas para salvaguardar alguno de los fines legítimos que menciona a continuación:

> «a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés

22. El título completo de ambas normas es; Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
23. Expresamente se afirma que se pretende garantizar que dicho intercambio no quede prohibido ni limitado por motivo de la protección de datos.

económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles».

La cantidad de fines individualizados como legitimadores de las limitaciones de estos derechos y la propia vaguedad de los términos utilizados para su mención (seguridad, interés público, protección de los derechos de otros...) conforman un marco amplio e indeterminado de eventual limitación de estos derechos, lo que tiene como consecuencia que para el ciudadano sea casi imposible prever los casos en los que puede ver sus derechos limitados.

De la misma vaguedad adolece la Directiva 2016/680, que se inicia con una declaración (art. 1.1) en el sentido de que el uso y tratamiento de los datos personales de las personas físicas se limitará a lo necesario para alcanzar alguna de las finalidades que lo legitiman y específicamente «la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública». Esta norma, a pesar de reconocer todos los derechos a los titulares de los datos (al plazo, al acceso a los mismos, a la rectificación...), sin embargo, establece también la posibilidad de limitar el ejercicio de estos derechos cuando supongan un obstáculo para las indagaciones, investigaciones o procedimientos oficiales o judiciales, o cuando el ejercicio de esos derechos perjudique la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, o implique un riesgo para la debida protección de la seguridad pública, la seguridad nacional o los derechos y libertades de otras personas (arts. 15, 16 Directiva). Con cláusulas tan vagas como las mencionadas se añaden escenarios aún más indeterminados en los que se habilita para la restricción de los derechos del particular que, por cierto en este marco, son tanto acusados y condenados, como víctimas

y testigos, cuyos datos también pueden verse restringidos si su ejercicio supone «un obstáculo para las indagaciones».

La jurisprudencia del Tribunal de Justicia de la Unión Europea

Una habilitación tan vaga y amplia para la restricción de estos derechos en el marco de una investigación judicial como la efectuada por el Reglamento y la citada Directiva hacen presagiar, por lo menos a los penalistas, que los Estados harán un uso amplio de dicha posibilidad. Pues cuando lo que está en juego es la investigación judicial de delitos, como el terrorismo, la pedofilia o el tráfico de drogas, los Estados están dispuestos a apurar todas las posibilidades legales, cuando no a sacrificar abiertamente los derechos de unos pocos en aras de los, en su opinión, intereses generales. No obstante, los Estados deberán tener en cuenta que el Tribunal de Justicia de la Unión Europea ya se ha ocupado de analizar la conformidad a la Carta de Derechos Fundamentales de la Unión Europea de algunas restricciones de los derechos de protección de datos en varias sentencias que, aunque se refieren a la legislación europea previa, establecen líneas interpretativas que son de aplicación general y que evidencian los problemas de una legislación conformada con cláusulas tan vagas como las contenidas en el Reglamento y la Directiva mencionadas.

Tres son las sentencias de cabecera en este ámbito a las que me voy a referir: la STJUE (Gran Sala) de 8 de abril de 2014 (Digital Rights); la STJUE de 21 de diciembre de 2016 (Tele2 Sverige Ab y otros); por último la STJUE de 2 de octubre de 2018, caso Ministerio Fiscal. Todas ellas se refieren a la conservación de los datos de las comunicaciones electrónicas y posterior acceso a los mismos como medio de investigación criminal. Como es sabido, uno de los derechos anudados a la protección de datos es el derecho a la destrucción de los mismos transcurrido un cierto tiempo, de modo que no se pueden conservar los datos y almacenarlos sin ningún límite. Sin embargo, la Directiva de 2002 en su art. 15.1 permitía al legislador nacional establecer excepciones a esa prohibición de conservación de datos cuando concurran razones de seguridad nacional, defensa, seguridad pública o necesidades derivadas de la prevención, investigación y persecución de delitos.

El caso de la STJUE de 2014, Digital Rights, se refiere a esta proveedora de servicios de telecomunicación que impugna la necesidad de conservar los datos, que establece la séptima parte de la Ley de Enjuiciamiento Criminal (Delitos de Terrorismo) de 2005 [Criminal Justice (Terrorist Offences) Act 2005. A ella se acumuló otra cuestión del Tribunal Constitucional austriaco que solicitó la anulación de un precepto que permitía el almacenamiento masivo de datos por razones de investigación criminal[24]. En esta cuestión se plantea entonces la compatibilidad de la Directiva 2006/24 con la Carta de Derechos Fundamentales de la Unión Europea por permitir tal almacenamiento masivo de datos[25].

---

24. Artículo 102a de la Ley de telecomunicaciones de 2003 (Tekommunikationsgesetz 2003), que fue introducido por la Ley federal por la que se modifica dicha Ley de telecomunicaciones (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011) con el fin de transponer la Directiva 2006/24 en el ordenamiento jurídico austriaco.
25. Los datos que deben conservar los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, con arreglo a los artículos 3 y 5 de la Directiva 2006/24, son, en particular, los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación, el equipo de comunicación de los usuarios y para identificar la localización del equipo

Pues bien, el Tribunal de Justicia anuló la directiva en 2014 al considerar que aunque era posible excepcionar este derecho –a la destrucción de los datos transcurrido un cierto tiempo–, sin embargo, no era legítimo hacerlo en los términos generales y amplios que permitía el art. 15.1 cuestionado. De acuerdo con el Tribunal de Justicia, dicha excepción, puesto que implica la limitación de un derecho fundamental, ha de interpretarse de manera restrictiva. Además, dado que se afectan derechos fundamentales, la limitación debe someterse a los requisitos de legitimidad establecidos por el art. 52 de la CDFUE, que, como sabemos son que la restricción esté prevista en la ley, que esta respete el contenido esencial del derecho y que sea proporcionada, es decir, que no implique más limitaciones que las estrictamente necesarias para alcanzar los objetivos propuestos.

A partir de este presupuesto, el Tribunal de Justicia razona que la conservación generalizada de los datos de tráfico de las comunicaciones, basada bien en la directiva 2006/24/CE o en el art. 15.1 de la Directiva 2001/58/CE supone una injerencia grave en los derechos fundamentales a la vida privada y familiar (art. 7 Carta) y protección de datos (art. 8 Carta). No obstante, reconoce que esta injerencia, aún grave, no incide en el contenido esencial del derecho vulnerándolo pues, de un lado, la medida no afecta al contenido de las comunicaciones sino a los datos de tráfico de la comunicación y, de otro, porque los proveedores de servicios mantienen ciertas obligaciones de salvaguarda y seguridad de los datos. En primer lugar, esta sentencia reconoce (par. 51) que a pesar de la importancia y trascendencia del objetivo perseguido con la limitación de los derechos a la protección de datos, la lucha contra la criminalidad grave, terrorismo, delincuencia organizada, etc., este objetivo no puede justificar por sí solo la injerencia. Por ello, al analizar el resto de los requisitos contemplados en el art. 52 CDFUE, el Tribunal de Justicia cuestionó la proporcionalidad de la imposición generalizada de una medida de este tipo con el propósito de facilitar/asegurar la lucha contra la delincuencia grave; en particular, sostuvo que la obligación de conservar todos los datos de todos los ciudadanos, cualquiera que sean y aunque no hayan tenido conexión ni sea previsible que tengan conexión futura con actividades delictivas, excede de los límites que la proporcionalidad requiere[26].

---

de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en particular, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que esta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto.

26. En la sentencia se señala (par. 56) que se deben conservar «todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el acceso a Internet, el correo electrónico por Internet y la telefonía por Internet» y de prácticamente toda la población europea, (p. 58) de modo que la restricción afecta a toda persona que utilice los servicios de telecomunicación. Y (par. 59) «no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves». Tampoco se delimita cuando los estados pueden acceder a esos datos, solo se mencionan los delitos graves y no se precisan (pár. 60), ni se delimitan las condiciones y procedimiento de dicho acceso (pár. 61). Tampoco se precisa el plazo de

Esta jurisprudencia fue reiterada en la STJUE de 21 de diciembre de 2016 en la que, además, expresamente se afirma que si es posible la conservación de datos con fines preventivos, aunque impone una serie de condiciones: que se haga de manera selectiva y con fines de lucha contra la delincuencia grave; que para ello es necesario que la normativa establezca criterios claros sobre la forma, las circunstancias y las garantías en la conservación de los datos frente a un uso irregular, incluido el plazo (par. 108); así mismo se requiere que la medida se refiera a personas que tengan una relación directa o indirecta con actividades criminales; que estas tienen que ser graves, y que el riesgo de las mismas debe ser asimismo un riesgo grave, señalándose incluso la necesidad de efectuar una delimitación del público afectado, por ejemplo, mediante el área geográfica en la que se aplicará (págs. 108-111, STJUE 21 de diciembre de 2016).

Igualmente resulta relevante señalar que esta sentencia impone (par. 120) garantías en el acceso a estos datos, conservados por más tiempo del general debido a su eventual conexión con actividades delictivas, por parte las autoridades nacionales. Así:

> «Para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales».

Es decir, que el Tribunal de Justicia de la Unión Europea exige una autorización previa para que la autoridad nacional acceda a estos datos, si bien esta autorización puede otorgarla una autoridad judicial o un órgano administrativo independiente; lo relevante, en todo caso, es que la autorización para el acceso a estos datos debe estar motivada expresamente en la necesidad de alcanzar los objetivos y en la proporcionalidad de tal acceso.

Una de las cuestiones abiertas a las que se refiere la tercera de las sentencias, es la relativa a cuándo estamos ante un delito grave, cuya investigación pueda legitimar, junto con otras condiciones, la limitación de este derecho. Se trata de una cuestión compleja que requiere una armonización en el marco europeo, pues como es sabido, los países europeos sancionan los delitos de manera muy diferente. Así, por ejemplo, Alemania cuenta con penas bastante moderadas para todos los delitos porque su máximo está en 15 años de prisión, de modo que podría considerar delitos graves los delitos sancionados con penas menores que otros países cuyas penas de prisión llegan hasta los 40 años.

La cuestión relativa a cuándo y bajo qué criterios podemos sostener que estamos ante un delito grave cuya investigación puede habilitar las excepciones a la protección de datos, fue planteada por el Ministerio Fiscal español en un asunto en el que la policía judicial había solicitado al juez de instrucción autorización para que la compañía proveedora del servicio de telefonía aportara ciertos datos de un

---

conservación atendiendo a la distinta entidad de los objetivos que lo justifican (par. 66) ni se contienen garantías suficientes de los proveedores de servicios para la conservación.

móvil; el juez denegó dicha autorización por entender que no se trataba de un delito grave ya que el delito investigado era un robo con violencia, cuya pena mínima es de 3 años que, conforme a la escala de penas del código penal español, no merece la consideración de pena grave, lo que determina que tampoco el delito se considere grave. El Ministerio Fiscal recurrió la resolución denegatoria y se acabó planteando la cuestión ante el Tribunal de Justicia de la Unión Europea.

En esta sentencia (Gran Sala, de 2 de octubre de 2018), el Tribunal de Justicia precisó que, en realidad, la normativa europea no exige que se investiguen delitos graves para que sea legítima la limitación de la prohibición de la conservación de los datos, sino que se trata de una exigencia de proporcionalidad de la medida que ha sido desarrollada por su jurisprudencia. Precisa que lo exigido es que a partir de que la injerencia en el derecho a la intimidad puede ser grave, los delitos investigados deberían ser también graves. Sin embargo, ello no significa que para justificar injerencias más leves en estos derechos se requiera siempre que el objetivo sea la investigación de delitos graves. Sostiene que si la injerencia no fuera tan grave, entonces podría estar justificada por la investigación de delitos en general, aunque no fueran graves. A partir de estas consideraciones analiza el contenido de los datos cuyo acceso se pedía y si, por consiguiente, dicho acceso constituía una injerencia básica o especialmente intensa en la intimidad, concluyendo que se trataba de una injerencia no muy intensa: como se pedía el acceso a los números de teléfono correspondientes a las tarjetas SIM así como a los datos personales o de filiación de los titulares de dichas tarjetas, tales como su nombre, apellidos y, en su caso, su dirección, el Tribunal afirma que dichos datos no permitían extraer conclusiones precisas sobre la vida privada de las personas:

> «Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados» (pár. 60).

Aunque el Tribunal de Justicia argumenta desde lógica de la proporcionalidad de toda medida restrictiva de un derecho fundamental y esta obedece a una lógica garantista y de coordinación de los derechos en juego, no dejo de pensar que cuando se abre la puerta a las excepciones a la protección de los derechos fundamentales tan sensibles como los datos personales resulta difícil contener estas excepciones en un marco razonable, pues aquí también opera la lógica de la pendiente inclinada y resbaladiza por la que, una vez que se pisa, resulta muy difícil no deslizarse. Por dicha razón, para evitar los peligros de ampliación del marco de las excepciones a la protección de los datos personales, creo que urge la elaboración de una legislación europea mucho más precisa que la existente, siendo este un reto, sin duda, asequible pues contamos ya con un conjunto normativo de referencia muy amplio en materia de cooperación judicial penal en la Unión Europea.

5

EL IMPACTO EN LAS RELACIONES LABORALES DEL DERECHO A LA PROTECCIÓN DE DATOS Y DE LOS DERECHOS DIGITALES

LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS Y GARANTÍA DE LOS DERECHOS DIGITALES Y SUS ESCLARECEDORES ANTECEDENTES JURISPRUDENCIALES

IGNACIO GARCÍA-PERROTE ESCARTÍN
Catedrático de Derecho del Trabajo (UNED)

5.1. EL DERECHO DE LA UNIÓN EUROPEA Y LOS ANTECEDENTES JURISPRUDENCIALES DE LA LEY ORGÁNICA 3/2018

5.1.1. El derecho de la Unión Europea

Un derecho «emergente», pero ya central de nuestro tiempo, es el derecho a la protección de datos personales.

Es indispensable citar, al efecto, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea («protección de datos de carácter personal»)[1], el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)[2] y,

1. «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan; 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación; 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».
2. Remito a J. R. Mercader, *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Madrid (Francis Lefebvre) 2019, 3ª ed, Mª. Eª Casas Baamonde, «Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», *Derecho de las Relaciones Laborales*, 2018, nº 2, J. L. Goñi, *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-ley 5/2018)*, *Albacete (Ed. Bomarzo)*, 2018, J., J. R. Mercader, *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia (Tirant lo Blanch) 2017, pp. 183 y ss. (también pp. 121 y ss.) C. H. Preciado, *El derecho a la protección de datos en el contrato de trabajo, adoptado al nuevo Reglamento 679/2016, de 27 de abril*, Madrid (Thomson Reuters Aranzadi), 2017 y E. Mª. Blázquez, *Aplicación práctica de la protección de datos en las relaciones laborales*,

en fin, los artículos 87 a 91 y conexos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

5.1.2. Jurisprudencia sobre el control del uso de los dispositivos digitales

Con carácter previo al análisis de la Ley Orgánica 3/2018, me parece interesante recordar el estado de la cuestión existente y la importante jurisprudencia recaída del TEDH, del TC y del TS[3]. La ausencia de regulación legal, entre nosotros, de los derechos digitales ha hecho que la jurisprudencia tuviera el protagonismo cuasi exclusivo en la configuración de esos derechos.

Lo primero que hay que recordar es que, con anterioridad a la Ley Orgánica 3/2018, ya la jurisprudencia exigía de las empresas que tuvieran una política clara sobre el uso de los medios informáticos y del control del respeto a dicha política y que dicha política hubiera sido comunicada a los empleados. Se trata de las SSTS 26 de septiembre de 2007, 8 de marzo de 2011, 6 de octubre de 2011 y 119/2018, 8 de febrero.

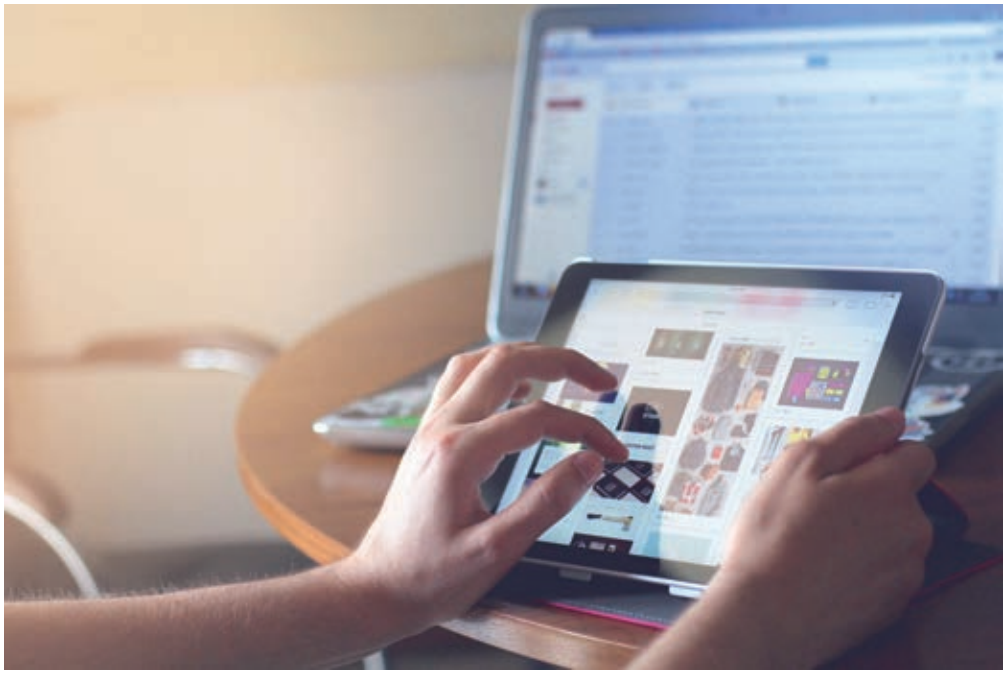
La manera de «romper» o modular la «expectativa de privacidad», a la que hace referencia, por ejemplo, la todavía importante STEDH, 3 de abril de 2007 (Copland), es precisamente la existencia de esa clara y comunicada política que puede incluir la prohibición del uso privado de los dispositivos o permitir un uso moderado y que, como se ha advertido, ha de advertir que la empresa fiscalizará que se cumple la política establecida. El criterio de que la prohibición de uso privado lleva implícita la facultad de control empresarial ha de entenderse matizada por la STEDH, 5 de septiembre de 2017 (Barbulescu II)[4].

Como es sabido, la jurisprudencia constitucional sentó desde el primer momento el criterio de que los trabajadores pueden ejercer sus derechos fundamentales en la empresa, si bien con las modulaciones o atemperaciones que sean imprescindibles o indispensables (principio de proporcionalidad) para preservar los derechos empresariales.

Madrid (Wolters Kluwer), 2018. De gran interés es el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017 por el Grupo de trabajo sobre protección de datos del artículo 29 de la Directiva 95/46/CE sobre protección de datos, y que tiene ya en cuenta el Reglamento 2016/679, que deroga aquella Directiva.

3. Remito, por todos, a J. Mª. Goerlich, «Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas» en Asociación de Letrados del Tribunal Constitucional, *El derecho a la privacidad en un nuevo entorno tecnológico*, Madrid (Centro de Estudios Políticos y Constitucionales), 2016, pp. 123 a 150, y J. R. Mercader, *El futuro del trabajo en la era de la digitalización y la robótica*, cit., pp. 121 y ss. Remito, asimismo, a A. Reis de Araujo, *El poder de control empresarial en la Web 2.0 y la dignidad del trabajador: el uso laboral de los dispositivos móviles y entornos colaborativos*, Albacete (Bomarzo), 2019; F. Valdés comenta este libro en «Nuevas tecnologías y derechos fundamentales de los trabajadores»,.cit. Me permito remitir, asimismo, a mi *Manual de Derecho del Trabajo*, Valencia (Tirant lo Blanch), 2019, 9ª ed., pp. 195 y ss. y 282 y ss.

4. Sobre esta STEDH son esenciales los trabajos de Mª. Eª Casas Baamonde, «Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», cit., y A. y E. Desdentado, «La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador», *Revista de Información Laboral*, 2018, núm. 1.



La jurisprudencia ha considerado que el artículo 20.3 del ET, en conexión con los artículos 33 y 38 de la CE, ampara el control empresarial en el que están en juego los derechos de los trabajadores reconocidos en los apartados 1, 2, 3 y 4 del artículo 18 de la CE.

Esta doctrina se fue construyendo en las SSTC 241/2012, 17 de diciembre, y 170/2013, 7 de octubre, STEDH 5 de septiembre de 2017 (Barbulescu II) y en las ya citadas SSTS, si bien conviene reiterar la cita de la STS 119/2018, 8 de febrero, porque ya tiene en cuenta la STEDH Barbulescu II.

La STC 241/2012, 17 de diciembre (con voto particular), enjuició un supuesto en el que existía una prohibición para uso privado, por lo que el TC aprecia que no había expectativa alguna de privacidad. Las demandantes de amparo instalaron un programa, en el que hacían comentarios despectivos de empleados y superiores, en un ordenador que era accesible a cualquiera, por lo que declara el TC que no podía estar en juego el secreto de las comunicaciones. A las trabajadoras se les impuso una sanción muy liviana.

Por su parte, la STC 170/2013, 7 de octubre, declaró que el acceso del empleador a determinados correos electrónicos del trabajador, que revelaban que transmitía indebidamente información reservada empresarial, no vulneró los derechos a la intimidad y al secreto de las comunicaciones del trabajador (artículo 18.1 y 3 CE). Para la STC 170/2013 el trabajador no podía tener una razonable expectativa de confidencialidad ni de privacidad (el convenio colectivo prohibía el uso privado) y el control empresarial respetó la proporcionalidad constitucionalmente exigida. En efecto, para el TC el control empresarial fue justificado, puesto que existían sospechas de un comportamiento irregular del trabajador; la medida era idónea para la finalidad pretendida por la empresa (si el trabajador revelaba a terceros datos empresariales de reserva obligada); y, en fin, la medida era necesaria, dado que el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial, sin que fuera suficiente el mero acceso a otros elementos de la comunicación como la identificación del

remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado. Finalmente –concluye el TC–, la medida podía entenderse como ponderada y equilibrada; al margen de las garantías con que se realizó el control empresarial a través de la intervención de perito informático y notario, el TC parte de que la controversia a dirimir se ceñía a los correos electrónicos aportados por la empresa como prueba en el proceso de despido.

La importante STEDH, Gran Sala, 5 de septiembre de 2017 (Barbulescu II), que revoca la previa STEDH 12 de enero de 2016 (Barbulescu I) –citada por la STC 39/2016, de 3 marzo, y que coincidía con la doctrina de las SSTC 241/2012 y 170/2013– concluye que a los tribunales rumanos les faltó determinar, en particular, si el Sr. Barbulescu había sido previamente advertido por su empleador de las posibilidades de que sus comunicaciones en Yahoo Messenger podrían ser monitorizadas (lo que debe hacerse antes de que se inicien las actividades de control) y, de otro lado, que no había sido informado de la naturaleza y extensión del control o del grado de intrusión en su vida privada y correspondencia. Adicionalmente, la STEDH, 5 de septiembre de 2017, entendió que los tribunales rumanos fallaron a la hora de determinar, en primer lugar, las concretas razones que justificaban la introducción de las medidas de control; y, en segundo lugar, si el empleador podía haber usado medidas menos intrusivas. La STEDH, 5 de septiembre de 2017, hace un acopio de la regulación supranacional, internacional y comparada, de las obligaciones positivas que emanan para los Estados del artículo 8 del CEDH y, aunque reconoce, de un lado, que «el empleador tiene un legítimo interés en asegurar el buen funcionamiento de la empresa y que ello puede hacerse estableciendo mecanismos para verificar que los empleados realizan sus tareas profesionales adecuada y diligentemente y, de otro, que los tribunales rumanos identificaron correctamente los intereses en presencia y los principios legales aplicables (necesidad, finalidad, transparencia, legitimidad, proporcionalidad y seguridad)», reprocha a los tribunales rumanos lo que se ha dicho. El TEDH rechaza las indemnizaciones por daños materiales y morales pedidas por el Sr. Barbulescu.

Posteriormente, la STEDH, 22 de febrero de 2018, (Libert c. Francia) (nº 588/13) consideró que no hubo ninguna violación de la vida privada de un empleado de los ferrocarriles franceses (SNCF, empresa pública, frente a lo que ocurría en el caso Barbulescu, lo que puede ser relevante desde la óptica de las obligaciones negativas y positivas de los Estados) que fue despedido de la empresa después de que la consulta de su ordenador profesional revelara el almacenamiento de archivos pornográficos y falsos certificados llevados a cabo en beneficio de terceros. El recurrente se quejaba de que su empleador había abierto sin su presencia ficheros del disco duro de su ordenador, lo que sería una vulneración del artículo 8 del CEDH. Los órganos judiciales franceses consideraron procedente su despido, razonando que, salvo que los identifique expresamente como personales (opción privado en *outlook*) (en este caso, se requiere en derecho francés la presencia del empleado), cabe presumir que los correos son profesionales. Y, si lo son, el empresario puede verlos; este es el derecho francés. El TEDH concedió mucha importancia al hecho de que el demandante no había identificado ese fichero como privado o personal en *outlook*.

En el caso, se establecía el uso estrictamente profesional, si bien se toleraba una utilización privada puntual; el recurrente contrarió «masivamente» estas instrucciones y no puede pretender –se dice con amparo en alguna sentencia francesa– que todo el disco duro es personal. El control estaba previsto por la ley (se afirma), y el TEDH examina la finalidad legítima (protección de los derechos de otro o de los

demás; en este caso los del empleador; se remite a Barbulescu, 127: interés legítimo del empresario en asegurar el buen funcionamiento de la empresa lo que le permite controlar a sus empleados) y la necesidad en una sociedad democrática (imperiosa y proporcionada). Al demandante, por sus funciones (encargado de la supervisión general), le es exigible un comportamiento ejemplar. El TEDH concluye que las autoridades internas no excedieron el margen de apreciación que les corresponde.

Es imprescindible mencionar, finalmente, la STS 119/2018, 8 de febrero, en la que el TS tiene ya en cuenta la STEDH, 5 de septiembre de 2017 (Barbulescu II). En un supuesto de despido (declarado procedente por el TSJ) en el que la empresa utilizó como prueba (aunque no única) determinados correos electrónicos del trabajador (que revelaban que había recibido dinero de un proveedor), el TS, corrigiendo en este extremo al TSJ, declara que el acceso a esos correos no vulneró ningún derecho fundamental del empleado reconocido en el artículo 18 de la CE. El TS tiene especialmente en consideración el hecho de que la empresa disponía de una política de utilización de medios informáticos en la que se limitaba el uso de tales medios, incluido especialmente el correo electrónico, para fines exclusivamente profesionales. Asimismo, las normas internas informaban con total claridad de la posibilidad de que la empresa supervisara o monitorizara la utilización de tales medios por los empleados. El trabajador conocía estas normas y las aceptaba diariamente al acceder al ordenador que tenía asignado.

Adicionalmente, la revisión del correo electrónico no se llevó a efecto de modo genérico o indiscriminado, sino tratando de encontrar elementos que permitieran seleccionar los correos a examinar, utilizando para ello palabras clave que permitieran inferir en qué correos podría existir información relevante para la investigación. De esta forma, el examen se limitó a los correos pertinentes para la investigación, disponibles en el correo corporativo del empleado, mediante el acceso al servidor alojado en las propias instalaciones de la empresa. Como consecuencia de todo ello, el TS entiende que la investigación se llevó a cabo en estricta conformidad con los cánones constitucionales de idoneidad, necesidad y proporcionalidad.

El TS afirma que las pautas sentadas por el TEDH son sustancialmente coincidentes con las emanadas del TC y del propio TS en su doctrina anterior a la STEDH Barbulescu II.

Todo ello lleva al TS a concluir que la conducta empresarial supera holgadamente el filtro del TEDH y que la revisión del correo electrónico efectuada fue un medio idóneo y necesario para completar la investigación de los hechos que fueron imputados en la carta de despido del trabajador. El TS entiende que la STC 170/2013, 7 de octubre, es una válida sentencia de contraste y cita también las SSTC 98/2000, 10 de abril, 186/2000, 10 de julio y 241/2012, 17 de diciembre, además de jurisprudencia del TC sobre el derecho a la intimidad.

Es interesante dar cuenta, finalmente, de la STS (Penal) 489/2018, 23 de octubre, lo que se hará con cierto detenimiento.

Afirma la STS (Penal) que la recién mencionada «STS –Sala 4ª– 119/2018, 8 de febrero, realiza una síntesis clara e íntegramente trasladable al ámbito penal del estado de la cuestión tras Barbulescu (II)».

La STS (Penal) de 2018 afirma que completa la conocida STS (Penal), 16 de junio de 2014.

La STS (Penal) de 2018 analiza la validez de las pruebas que se habían obtenido del ordenador de un directivo (i) respecto del que existían vehementes sospechas de deslealtad, (ii) con presencia notarial y medios técnicos para hacer una copia espe-

jo del disco duro, (iii) utilizando una herramienta informática metódica y selectiva para no realizar un acceso indiscriminado, y (iv) adoptando cautelas para asegurar la fidelidad del copiado.

La STS (Penal) de 2018 aplica la doctrina del caso Barbulescu II y, a pesar de valorar que se utilizaron métodos informáticos especialmente poco invasivos y selectivos, concluye que, al no existir advertencia de que el ordenador había de ser usado exclusivamente para los fines de la empresa y dado que no le constaba al empleado que la empresa se reservaba la potestad de su examen, la falta de consentimiento del titular o, en su defecto, de la autoridad judicial, viciaba la validez de la prueba, dejándola sin efecto.

El despido fue declarado procedente por el orden social de la jurisdicción; el delito atribuido al empleado era el continuado de apropiación indebida.

La STS (Penal) de 2018 parte de que «el reconocimiento previo, explícito o implícito, de esa facultad de empresario constituye el *punctum dolens* la clave, en el ámbito de las relaciones laborales. En una investigación penal lo será la autorización judicial o el consentimiento actual» (FJ 7).

La STS (Penal) de 2018 menciona, entre otras, las STEDH Barbulescu II, Libert y López Ribalda I (pero téngase en cuenta que esta sentencia ha sido revocada por la STEDH, Gran Sala, de 17 de octubre de 2019, López Ribalda II), rechazando, respecto de Barbulescu II, que «sea totalmente rupturista con los criterios que han ido cristalizando en nuestra jurisprudencia», pero «aporta y concreta al establecer con diáfana claridad parámetros de inexcusable respeto empujando a nuevas modulaciones y matizaciones que ya han aparecido en la jurisprudencia laboral (STS –Sala 4ª– 119/2018, de 8 de febrero), que realiza –como ya se ha avanzado que afirma la STS (Penal) de 2018– una síntesis clara e íntegramente trasladable al ámbito penal del estado de la cuestión tras Barbulescu».

La STS (Penal) de 2018 pondera los bienes en conflicto. De una parte, el interés del empresario en evitar o descubrir conductas desleales o ilícitas del trabajador, interés que prevalecerá solo si se atiene a ciertos estándares que han venido a cono-

cerse como el test Barbulescu. La STS (Penal) enuncia los criterios de ponderación relacionados con la necesidad y utilidad de la medida, la inexistencia de otras vías menos invasivas; la presencia de sospechas fundadas, etc. Algunos se configuran como premisas de inexcusable concurrencia. En particular –afirma la STS (Penal)–, no cabe un acceso inconsentido al dispositivo de almacenamiento masivo de datos «si el trabajador no ha sido advertido de esa posibilidad y/o, además, no ha sido expresamente limitado el empleo de esa herramienta a las tareas exclusivas de sus funciones dentro de la empresa (los usos sociales admiten en algún grado y según los casos, como se ha dicho, el empleo para fines personales, creándose así un terreno abonado para que germine una expectativa fundada de privacidad que no puede ser laminada o pisoteada)».

El resto de factores de ponderación entrarán en juego para inclinar la balanza en uno u otro sentido solo si se cuenta con ese presupuesto. En otro caso, «habrá vulneración aunque exista necesidad, se use un método poco invasivo, etc.» (FJ 9).

«Esta es la clave –razona la STS (Penal)– que nos permite resolver este asunto. Podrían existir razones fundadas para sospechar y entender que el examen del ordenador era una medida proporcionada para esclarecer la conducta desleal y evaluar los perjuicios. Se buscó, además, una fórmula lo menos invasiva posible. Pero faltaba un *prius* inexcusable, concluye la STS (Penal)».

«Si existiese esa expresa advertencia o instrucción en orden a la necesidad de limitar el uso del ordenador a tareas profesionales, (de la que podría llegar a derivarse una anuencia tácita al control o, al menos, el conocimiento de esa potestad de supervisión) y/o además alguna cláusula conocida por ambas partes autorizando a la empresa a medidas como la aquí llevada a cabo; o, si se hubiese recabado previamente el consentimiento de quien venía usando de forma exclusiva el ordenador (en caso de negativa, nada impedía recabar la autorización necesaria) pocas dudas podrían albergarse sobre la legitimidad de la actuación indagatoria llevada a cabo por la empresa. Pero en las circunstancias en que se llevó a cabo hay que afirmar que el ordenamiento ni consiente, ni consentía en la fecha de los hechos, tal acción intrusiva por ser lesiva de derechos fundamentales» (FJ 10).

«Lo que vicia –en suma– la prueba es el acceso no legítimo». La ilegitimidad «no deriva del contenido obtenido, ni de la forma de acceso más o menos intrusiva, sino del mismo acceso inconsentido y no advertido previamente» (FJ 11) [5].

Subraya la STS (Penal) que la jurisprudencia ha situado la clave de la legitimidad de la injerencia empresarial en «la ausencia de toda expectativa de confidencialidad por parte del trabajador que sufre la intromisión que puede basarse en una cláusula

5. Por lo que se refiere a si los correos habían sido ya abiertos o no, cuestión relevante para la STS (Penal) de 2014, la STS (Penal) de 2018, declara que «tampoco se debe reputar decisiva a estos efectos la difícil cuestión de dilucidar si todos los mails examinados habían sido ya recepcionados o tuvieron que abrirse algunos antes de que hubiese accedido a ellos el acusado. Aparte de las dificultades –casi imposibilidad– de determinarlo, no es dato al que aquí haya que otorgar relevancia decisoria. No puede descartarse la presencia de correos sin abrir. Y tampoco en estos casos –registro de dispositivos de almacenamiento masivo de datos– ese elemento accesorio puede convertirse en la piedra de toque que traiga la solución. No se atiene a parámetros de lógica esa distinción. Adquiere pleno sentido en los procesos de comunicación postales (interceptación antes de que se cierre el proceso de comunicación o una vez agotado este: la carta ya abierta que se guarda en un bolsillo es diferente –muy diferente– a la carta que se abre antes de llegar a su destinatario); pero esos moldes no son trasladables sin más a las comunicaciones vía telemática o telefónica».

contractual o en una advertencia del empresario o en la legítima instrucción expresa de limitar el uso del dispositivo a fines laborales. La existencia de un precepto incorporado al convenio del sector donde se prohíbe el uso personal de los instrumentos informáticos, la suscripción de una cláusula que reserva al empresario esa facultad o, en fin, la comunicación, por uno u otro medio, del uso de mecanismos tecnológicos de fiscalización –sigue razonando la STS (Penal)–, difuminan el espacio de exclusión del trabajador».

La STS (Penal) entiende que «ninguno de esos presupuestos legitimadores aparece aquí». La STS (Penal) concluye que «en el caso presente, a la vista de la jurisprudencia existente y predominante en el momento de la actuación empresarial cuya licitud fiscalizamos ahora, se podía y debía haber extremado la cautela: no existiendo advertencia de que el ordenador había de ser usado exclusivamente para los fines de la empresa y no constando al empleado que la empresa se reservaba la potestad de su examen, por mucho que se utilizasen métodos informáticos especialmente poco invasivos y selectivos, constituía un cierto atrevimiento (una indiligencia), no recabar antes el consentimiento del titular o, en su defecto, la autoridad judicial. Regía ya un cuerpo de doctrina jurisprudencial que alertaba sobradamente sobre la dudosa legalidad de esa actuación. Algo de osadía se aprecia en la iniciativa adoptada por la empresa», lo que le lleva a declarar que la prueba «no es rescatable; no puede utilizarse» (FJ 15).

5. 1.3. Jurisprudencia sobre videovigilancia

Por lo que se refiere a la videovigilancia empresarial, las sentencias relevantes son las SSTC 98/2000, 10 de abril, y 186/2000, de 10 julio, y, especialmente, la STC (Pleno) 39/2016, 3 de marzo, que rectifica la STC 29/2013, 11 de febrero, y la STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II), que revoca la STEDH 9 de enero de 2018 (López Ribalda I)[6].

La STC 186/2000 consideró compatible con la CE el establecimiento de un circuito cerrado de captación de imágenes únicamente en el puesto de trabajo (la caja) en el que se sospechaba que se estaban cometiendo irregularidades. La STC 186/2000 declaró que la medida era justificada, idónea, necesaria y equilibrada.

Por el contrario, la STC 98/2000 consideró incompatible con la CE un sistema de grabación de sonido que permitía, en un casino, en el que ya se grababan las imágenes, escuchar, además, las conversaciones de los trabajadores.

La STC (Pleno) 39/2016, de 3 marzo (con votos particulares), rectificando la STC 29/2013, de 11 febrero (también con voto particular), rechazó que se hubieran vulnerado los derechos a la intimidad y a la protección de datos de carácter personal (artículo 18.1 y 4 de la CE) por la utilización de imágenes captadas por las cámaras de videovigilancia instaladas en la empresa con la finalidad de supervisión laboral (había sospechas de que algún trabajador se estaba apropiando de dinero de la caja), entendiéndose cumplido el deber de información previa (que forma parte del contenido esencial del derecho a la protección de datos) a través del distintivo exigido

6. Sobre esta primera STEDH López Ribalda I es esencial igualmente el trabajo Mª. Eª Casas Baamonde, «Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral», cit.

por la Instrucción 1/2006, 8 noviembre, de la AEPD, colocado en el escaparate de la tienda, sin que haya que especificar la «finalidad exact» que se le ha asignado a ese control y, respecto del derecho a la intimidad, el TC declara que se observó estrictamente el principio de proporcionalidad. La STC 39/2016 tiene muy en cuenta la existencia de sospechas para justificar la instalación de un sistema de videovigilancia. Creo que este es un elemento relevante pues una cosa es un sistema de videovigilancia instalado con carácter permanente (y no ante la existencia de concretas sospechas) y otra un sistema de videovigilancia instalado *ad hoc* ante la existencia de sospechas, sistema que será en principio temporal y no permanente. Especialmente tras la Ley Orgánica 3/2018, en el primer caso habrá que proporcionar la información previa, expresa, clara y concisa que exige el párrafo primero del artículo 89.1 de la Ley Orgánica 3/2018, mientras que en el segundo valdrá el dispositivo al que se refiere el párrafo segundo del artículo 89.1 de la Ley Orgánica 3/2018 y al que se refería la STC 39/2016. Al cabo, y desde este punto de vista, las SSTC 29/2013 y 39/2016 podrían ser hasta compatibles.

Las SSTS, 7 de julio de 2016, 31 de enero de 2017,1 de febrero de 2017 y 2 de febrero de 2017 aplican ya el criterio de la STC 39/2016. La STS, 2 de febrero de 2017, es interesante porque fueron otros trabajadores quienes se quejaron y denunciaron al trabajador despedido. De interés es la STS 21/2019, de 15 de enero que, advierte que en el supuesto enjuiciado por la sentencia recurrida no se cumplió con el deber de información, al contrario de lo que sucedió en la STC 39/2016, por lo que aprecia falta de contradicción porque la sentencia recurrida resolvió conforme a la STC 39/2016, que era la sentencia esgrimida de contraste.

La muy relevante STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II), enjuicia un supuesto de vídeo vigilancia secreta de cajeras en un supermercado español entendiendo que, frente a lo que habría considerado inicialmente el propio TEDH en López Ribalda I (STEDH 9 de enero de 2018 que ahora se revoca), no se vulneró su derecho a la vida privada (artículo 8 CEDH), y no solo su derecho a un juicio justo (artículo 6 CEDH), que ya López Ribalda I había rechazado que se hubiera infringido. La vídeo vigilancia oculta tuvo por finalidad comprobar las sospechas de

hurto. Las cuatro demandantes fueron despedidas, fundamental (aunque no únicamente), en base a las grabaciones de vídeo. Los tribunales laborales españoles admitieron como prueba las grabaciones y declararon la procedencia de los despidos; por su parte, el TC no admitió los recursos de amparo. Ante las sospechas de hurto, el empresario instaló cámaras visibles y cámaras ocultas. La empresa informó a los trabajadores de la instalación de las cámaras visibles, pero no de las cámaras ocultas. Todos los trabajadores sospechosos de hurto fueron convocados a entrevistas individuales en las que se les mostraron los vídeos. Las cámaras habían filmado a las trabajadoras mientras ayudaban a los clientes y a las compañeras a sustraer artículos y a sustraerlos ellas mismas.

La STEDH López Ribalda II parte de que los tribunales españoles identificaron y ponderaron adecuadamente los derechos de las trabajadoras (el respeto a su vida privada ex artículo 8 CEDH) y los de la empresa (la protección de su propiedad y la buena marcha de su empresa), examinando la justificación de las medidas de videovigilancia. Respecto del argumento de que las trabajadoras no habían sido advertidas de la vigilancia, a pesar de que así lo establecía la legislación española vigente en ese momento, el TEDH declara que la medida estaba justificada por la existencia de sospechas legítimas de graves irregularidades y pérdidas, por la que la medida fue proporcionada y legítima. La STEDH López Ribalda II señala que los principios sentados en el caso Barbelescu II son aplicables a la videovigilancia en el lugar de trabajo. Los tribunales internos tuvieron en cuenta la sospecha de robo, que las cámaras enfocaban exclusivamente a las cajas y que las empleadas trabajaban en un área abierta al público. La STEDH López Ribalda II hace una distinción entre el grado de intimidad que un empleado puede esperar dependiendo de dónde trabaje: la expectativa puede ser muy alta en lugares como baños o vestuarios, donde se puede justificar una prohibición total de la videovigilancia; puede ser alta en espacios de trabajo cerrados, como oficinas; y es, sin embargo, reducida en lugares visibles o accesibles para compañeros o para una amplia audiencia. También tiene en cuenta el TEDH que la vigilancia duró solo diez días, que las grabaciones fueron vistas por un número reducido el número de personas, que no se utilizaron para ningún otro fin que para determinar quiénes eran los responsables de las sustracciones y, especialmente, que ninguna otra medida hubiera permitido alcanzar dicho objetivo legítimo.

En cuanto a la falta de advertencia o notificación previa de la vídeo vigilancia, la STEDH López Ribalda II afirma que existe un amplio consenso internacional sobre la obligación de esa información previa, de manera que sólo una imperativa protección de los intereses públicos o privados importantes podría justificar la falta de información previa, lo que tiene como consecuencia que, si bien no cabe aceptar que la más mínima sospecha de que las irregularidades han sido perpetradas por los empleados pueden justificar una videovigilancia secreta por parte del empleador, la sospecha razonable de que se habían cometido graves irregularidades y el alcance de las mismas producidas en este caso pueden considerarse justificaciones serias, especialmente si, como ocurría en el caso, se sospechaba de la acción concertada de varios empleados. Por lo demás, las trabajadoras tenían a su alcance otros medios (que no utilizaron) para solicitar la reparación de la presunta violación de sus derechos en virtud de la legislación nacional de protección de datos.

La STEDH López Ribalda II descarta, finalmente, que la videovigilancia haya vulnerado el derecho a un juicio justo (artículo 6 CEDH), toda vez tuvieron la oportunidad de oponerse a la utilización de pruebas y los tribunales nacionales argumen-

taron ampliamente sus resoluciones. El TEDH tiene en cuenta que las grabaciones no eran los únicos elementos de juicio (se tuvieron en cuenta otras pruebas), y que las trabajadoras no refutaron su autenticidad y exactitud.

5.2. LA LEY ORGÁNICA 3/2018: EL USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL; LAS OBLIGACIONES EMPRESARIALES

En este contexto y con estos importantes antecedentes, se ha promulgado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en cuyos artículos 87 a 91[7], y preceptos conexos, me voy a centrar[8]. La novedad de la Ley Orgánica 3/2018 espero que justifique la superior extensión de este apartado del trabajo en relación con los otros.

En los apartados 1 y 2 del artículo 87 (denominado «derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral») de la Ley Orgánica 3/2018 se proclama, de un lado, en el apartado 1, el derecho de los trabajadores (y de los empleados públicos) a «la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador» y, de otro, en el apartado 2, el derecho (aunque se evita utilizar esta palabra) del empleador a «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»[9]. A destacar que el derecho de acceso empresarial se circunscribe estrictamente («a los solos efectos») a «controlar el cumplimiento de las obligaciones laborales (o estatutarias)» y a «garantizar la integridad» de los dispositivos. También hay que mencionar que el derecho del trabajador se ciñe a la protección de su intimidad sin que se mencione ni el propio derecho a la protección de datos ni tampoco otros derechos proclamados en el artículo 18 CE[10].

---

7. A destacar que los artículos 87 y 88 de la Ley Orgánica 3/2018 no se mencionan por el artículo 2 de esa Ley Orgánica, por lo que no se considera que se refieran al tratamiento de datos personales.
8. Remito con carácter general a los libros de J. R. Mercader, *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, cit., 3ª ed., especialmente pp. 127 y ss., y C. H. Preciado, *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, Thomson Reuters, Aranzadi, 2019, con prólogo de A. V. Sempere. También es de obligada cita J. García Murcia e I. Rodríguez Cardo, «la protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo, *Revista Española de Derecho del Trabajo*, enero 2019, núm. 216.
9. Sobre la ausencia de mención a los empleados públicos en el apartado 2 del artículo 87 de la Ley Orgánica 3/2018, al contrario de lo que sucede en el apartado 1 del precepto –que todo indica que es una omisión involuntaria–, se remite a C. H. Preciado, *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, cit., pp. 115 y ss.
10. Y es curioso, porque «la protección de datos se come a la intimidad», como decíamos con un punto de exageración J. Mercader y yo en «La protección de datos se come a la intimidad: la doctrina de la sentencia del TEDH de 5 de septiembre de 2017 (caso Barbulescu v. Rumania; nº 61496/08; Gran Sala)», *Revista de Información Laboral*, núm. 10/2017. En el artículo se cita a D. Cordova y L. M. Díez Picazo en su luminoso trabajo, «Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico», en Asociación de Letrados del Tribunal Constitucional, *La privacidad en un nuevo entorno tecnológico* , Madrid, CEPC, 2016, «la protección de datos, si bien nació tímidamente, se ha convertido en un agujero negro que lo absorbe todo y no deja escapar nada de su entorno».Como dice expresivamente Y. N. Harari, «quienes

Podría llamar la atención, así, el aparente «reduccionismo» en este extremo de la Ley Orgánica 3/2018[11]. Es verdad que, desde la perspectiva del tratamiento de datos *ex* artículo 2 de la Ley Orgánica 3/2018, ya se ha dicho que los artículos 87 y 88 de dicha Ley Orgánica no se mencionan por aquel artículo, al contrario de lo que sucede con los artículos 89 y 90; pero también es cierto que también los artículos 89 y 90 solo mencionan, al igual que el artículo 87, el derecho a la intimidad.

El apartado 3 del artículo 87 de la Ley Orgánica 3/2018 crea una primera obligación empresarial consistente en que los empleadores «deberán establecer criterios de utilización de los dispositivos digitales». Esta es, en consecuencia, una tarea que deben acometer aquellas empresas que no lo hayan hecho, aunque sabido es que en muchas empresas ya se cuenta con estos criterios de utilización en forma de protocolos, códigos de conducta, etc. Pero habrá que revisar, desde luego, si estos códigos de conducta se adecúan a la Ley Orgánica 3/2018. Ha de tenerse en cuenta, entra otras cuestiones, que en la «elaboración» de los criterios de utilización deberán «participar» los representantes de los trabajadores (artículo 87.3, último inciso, de la Ley Orgánica 3/2018).

El significado del término participación no es unívoco. Parece claro que es algo distinto y que se quiere diferenciar de la «previa audiencia» de los representantes de los trabajadores prevista para la política interna empresarial sobre derecho a la desconexión digital del artículo 88.3 de la Ley Orgánica 3/2018. También hay que recordar que nuestra legislación diferencia entre información, consulta y participación en la empresa (artículo 4.1 g) ET). Por su parte, el artículo 129.2 de la CE dispone que «los poderes públicos promoverán eficazmente las diversas formas de participación en la empresa» y el artículo 61 del ET, que lleva en su título la palabra «participación», literalmente acaba afirmando que «... los trabajadores tienen derecho a participar en la empresa a través de los órganos de representación regulados en este Título», si bien es cierto que se precisa que lo es «de conformidad con lo dispuesto en el artículo 4 (ET) y sin perjuicio de otras formas de participación».

---

poseen los datos poseen el futuro» (*21 lecciones para el siglo XXI*, cit. p. 96). O, en las palabras igualmente expresivas, de J.R. Mercader, el *big data* es el «oro» de la economía digital (J. R. Mercader, El futuro del trabajo en la era de la digitalización y la robótica, cit., p. 183).

11. C. H. Preciado, Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales, cit., p. 114.

En el Derecho de la Unión Europea la expresión «participación» se reserva al eventual derecho del órgano de representación de los trabajadores o de los representantes de los trabajadores de «elegir o designar a determinados miembros del órgano de administración o de control de la sociedad» o de «recomendar u oponerse a la designación de una parte o de todos los miembros del órgano de administración o de control de la sociedad» (artículo 2 k) de la Directiva 2001/86/CE, de 8 de octubre de 2001, del Consejo, que completa el Estatuto de la Sociedad Anónima Europea en lo que respecta a la implicación de los trabajadores. Y, con excepción de aquella Directiva y de este Estatuto, las demás normas de la Unión Europea se refieren solo a la información y consulta (artículo 27 de la Carta de los Derechos Fundamentales de la Unión Europea y la Directiva 2002/14/CE, de 11 de marzo de 2002, del Consejo y del Parlamento Europeo, que establece un marco general relativo a la información y consulta de los trabajadores de la Comunidad Europea; igualmente lo hace la Directiva 2009/38/CE, del Parlamento Europeo y del Consejo, de 6 de mayo de 2009, sobre la constitución de un comité de empresa europeo o de un procedimiento de información y consulta a los trabajadores en las empresas y grupos de dimensión comunitaria)[12].

Creo que el panorama anterior revela que, en efecto, el significado de la participación de los representantes de los trabajadores del artículo 87.3 de la Ley Orgánica 3/2018 no es del todo claro. No es solo información, y por otro lado se ha rehuido la utilización de la palabra consulta[13], pero de ahí no creo que pueda interpretarse que se trata de un supuesto de negociación colectiva en sentido estricto impeditivo de la unilateralidad empresarial. Materialmente se trata más bien de consulta[14] y, como máximo se podrá asemejar a un periodo de consultas en el sentido de los artículos 40, 41, 47, 51 y 82.3 del ET que admiten, tras la negociación de buena fe, una decisión empresarial unilateral.

Los criterios de utilización de los dispositivos digitales deberán «respetar» en todo caso «los estándares mínimos de protección de su (de los trabajadores ha de entenderse) intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente».

A subrayar esta apelación a los «estándares mínimos de protección», y, más todavía, a los «usos sociales», mención esta última que recuerda a las referencias que hace la importante STS, 26 de septiembre de 2007 (r. 966/2006) al «hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores», tolerancia que crea «una expectativa también general de confidencialidad en esos usos». No está de más recordar aquí la consideración que se hace en la STEDH, 5 de septiembre de 2017 (Barbulescu II) de que las instrucciones empresariales «no pueden reducir a cero (o a la nada) la vida social privada en los lugares de trabajo», en el sentido de que «el respeto de la vida privada y de la correspondencia (artículo

12. Es verdad que el Tratado de Funcionamiento de la Unión Europea diferencia entre «la información y consulta a los trabajadores» [(letra e) del artículo 153.1] y «la representación y la defensa colectiva de los intereses de los trabajadores y empresarios, incluida la cogestión» [(letra f) del artículo 153.1].
13. La información y la consulta se definen, como se sabe, en el artículo 64.1 del ET.
14. En el mismo sentido, C. H. Preciado, *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre* de *Protección de Datos y Garantía de los Derechos digitales*, cit., pp. 119 y ss.

8 del Convenio Europeo de Derechos Humanos) continúa existiendo, aunque puede ser limitado en la medida en que ello sea necesario».

Por su parte, la referencia al necesario respeto de «los derechos reconocidos constitucional y legalmente», que puede parecer obvia, recuerda que los criterios de utilización establecidos por la empresa tienen como límite aquellos derechos, que constitucionalmente no se circunscriben tan solo a la intimidad, y que lógicamente habrá que respetar de conformidad con su definición internacional, supranacional, constitucional y legal y con su integración jurisprudencial igualmente internacional, supranacional, constitucional y del Tribunal Supremo.

El párrafo segundo del apartado 3 del artículo 87 de la Ley Orgánica 3/2018 se preocupa de establecer qué debe hacerse en el supuesto de que se «haya admitido» el «uso» de los dispositivos digitales para «fines privados». Implícitamente se está admitiendo, en consecuencia, que como viene aceptando sin problemas nuestra jurisprudencia (elocuente es al respecto la STS 119/2018, de 8 de febrero), los criterios de utilización empresariales pueden prohibir el uso de aquellos dispositivos para fines privados.

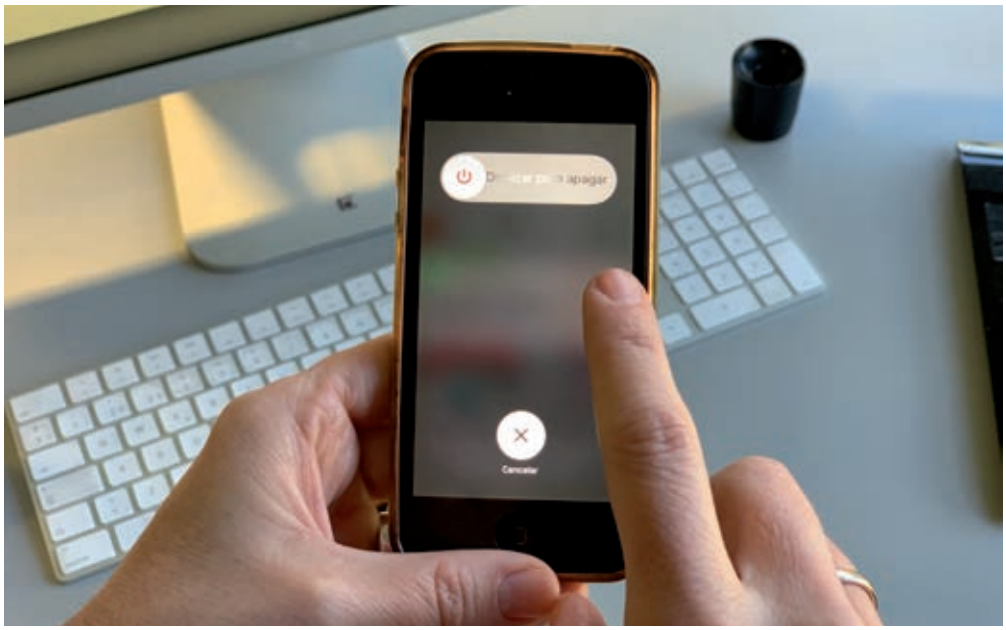
En fin, el caso es que, en el supuesto de que los criterios de utilización empresariales hayan admitido el uso de los dispositivos digitales con fines privados, «el acceso por el empleador al contenido» de dichos dispositivos «requerirá que se especifiquen (ha de entenderse que en los criterios de utilización empresariales) 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» (artículo 87.3, párrafo segundo, de la Ley Orgánica 3/2018).

El cuarto y último párrafo del apartado 3 del artículo 87 de la Ley Orgánica 3/2018 dispone que «los trabajadores deberán ser informados de los criterios de utilización» de los dispositivos digitales establecidos por la empresa.

Esta obligación de información a cargo de la empresa, y el correlativo derecho del trabajador a ser informado, son verdaderamente claves, siendo fundamental para los empleadores cumplir con esta obligación. Baste con mencionar que la ausencia de toda información (o de la previa o adecuada información) fue el «error» empresarial (el «pecado capital», podría decirse) que se cometió en los despidos y en los supuestos enjuiciados por la STS, 26 de septiembre de 2007, la STEDH, 5 de septiembre de 2017 (Barbulescu II), la STS (Penal) 489/2018, de 23 de octubre, y la STS 21/2019, de 15 de enero. Y, por el contrario, fue el «acierto» empresarial, entre otros, del despido y del supuesto enjuiciado por la STS 119/2018, de 8 de febrero. La Ley Orgánica 3/2018 hace ulteriores referencias, de las que se dará debida cuenta más adelante, a la obligación empresarial de informar a los trabajadores. Como dice la Comisión Mundial sobre el Futuro del Trabajo de la OIT, «se debería informar a los trabajadores de cualquier control que se realice en el lugar de trabajo»[15].

Hay que recordar, adicionalmente, que, aunque el artículo 87.3, párrafo último, de la Ley Orgánica 3/2018 no lo explicita, de conformidad con la jurisprudencia, especialmente con la STEDH, 5 de septiembre de 2017 (Barbulescu II), la obligación empresarial de información no es solo de los criterios de utilización de los dispositivos digitales, sino que se extiende a que se tenga que informar adicionalmente

15. Comisión Mundial sobre el Futuro del Trabajo, Trabajar para un futuro más prometedor, OIT, enero 2019, cit., p. 46,



de que la empresa controlará («monitorizará») que los trabajadores cumplen con aquellos criterios de utilización, incluso –tras la STEDH 5 de septiembre de 2017 (Barbulescu II) y la STS 119/2018, de 8 de febrero, es más seguro hacerlo así, frente a lo que había entendido la STS, 6 de octubre de 2011– en los supuestos de prohibición de uso para fines privados.

5.3. EL DERECHO A LA DESCONEXIÓN DIGITAL Y LAS OBLIGACIONES EMPRESARIALES

El artículo 88 de la Ley Orgánica 3/2018 reconoce el «derecho a la desconexión digital en el ámbito laboral»[16]. Seguramente sea este el derecho «estrella», o al menos el más novedoso, de la vertiente laboral de Ley Orgánica 3/2018. Como dice el Preámbulo de la Ley Orgánica 3/2018, dentro del Título X («Garantía de los derechos digitales») de dicha Ley Orgánica, «ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral».

Hay que recordar, no obstante, que el artículo 88 de la Ley Orgánica 3/2018 tiene carácter de ley ordinaria y no de ley orgánica (disposición final primera de la Ley Orgánica 3/2018) y que el artículo 2 de la Ley Orgánica 3/2018 no menciona el artículo 88 de esa Ley Orgánica. Por lo demás, la vulneración del derecho a la desconexión digital no se tipifica como infracción en el título IX («Régimen sancionador») de la Ley Orgánica 3/2018, sin que tampoco la Agencia Española de Protección de Datos pueda conocer de las reclamaciones sobre dicho derecho porque no protege datos personales (artículo 65.2 de la Ley Orgánica 3/2018) y aunque a aquella Agencia le competa supervisar la aplicación de la esta Ley Orgánica (artículo 47 de la Ley Orgánica 3/2018).

16. Se remite a Mª. T. Igartua, «El derecho a la desconexión en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales», *Revista de Trabajo y Seguridad Social*, núm. 432, marzo 2019, pp. 61-87.

El derecho a la desconexión digital se reconoce a los trabajadores (y a los empleados públicos) «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» (artículo 88.1 de la Ley Orgánica 3/2018). Desde un punto de vista finalista, el derecho a la desconexión digital se conecta –valga el juego de palabras–, de un lado, con el tiempo de descanso –mencionándose expresamente los permisos y vacaciones– y, de otro, con la intimidad personal y familiar.

Las modalidades de ejercicio del derecho de desconexión digital han de atender a la «naturaleza y objeto de la relación laboral» y han de potenciar el «derecho a la conciliación de la actividad laboral y la vida personal y familiar» (artículo 88.2 de la Ley Orgánica 3/2018). La referencia a la naturaleza y objeto de la relación laboral parece especialmente afortunada, toda vez que, en efecto, a los efectos de «las modalidades de ejercicio» del derecho de desconexión digital, importan mucho la naturaleza y el objeto de cada relación laboral concreta.

El artículo 88.2 de la Ley Orgánica 3/2018 menciona expresamente «la negociación colectiva o, en su defecto, (el acuerdo) entre la empresa y los representantes de los trabajadores». Las modalidades de ejercicio del derecho a la desconexión digital han de sujetarse a lo establecido en aquella, o, en su defecto, a este acuerdo entre empresa y representantes de los trabajadores. Hay que destacar, así, esta expresa referencia –e invitación, cabría decir– a la negociación colectiva.

Sea como fuere, «previa audiencia de los representantes de los trabajadores», el empleador está obligado a elaborar «una política interna dirigida a (los) trabajadores» sobre el derecho a la desconexión digital (artículo 88.3 de la Ley Orgánica 3/2018). El precepto legal establece así una segunda obligación empresarial consistente en la exigencia de elaborar esa «política interna».

Como se ha avanzado, el empleador ha de cumplir con su obligación «previa audiencia de los representantes de los trabajadores». En el derecho de desconexión digital hay, así, «previa audiencia» (artículo 88.3 de la Ley Orgánica 3/2018), mientras que los criterios de utilización de los dispositivos digitales se elaboran con participación de los representantes de los trabajadores (artículo 87.3 de la Ley Orgánica 3/2018).

La política interna empresarial dirigida a los trabajadores ha de incluir a «los que ocupen puestos directivos» (artículo 88.3 de la Ley Orgánica 3/2018). La Ley Orgánica es consciente de que los directivos están entre los colectivos más expuestos a la conectividad permanente.

En la política interna a la que se viene haciendo referencia se han de definir «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» (artículo 88.3 de la Ley Orgánica 3/2018).

La política interna se ha de ocupar, así, de definir (i) las modalidades de ejercicio del derecho a la desconexión y (ii) las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. A subrayar la preocupación de la Ley 3/2018 porque se realizan estas acciones de formación y sensibilización encaminadas a conseguir que exista un «uso razonable» de las herramientas tecnológicas que evite el riesgo de «fatiga informática». La expresa mención a la «fatiga informática» y su calificación de «riesgo» son especialmente destacables.

En particular, la política interna ha de 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» (artículo 88.3 de la Ley 3/2018).

Por su parte, la nueva redacción del artículo 49.6 del Código de Comercio, dada al precepto por la ya citada Ley 11/2018, de 28 de diciembre, incorpora la «implantación de políticas de desconexión laboral» dentro de la información no financiera a facilitar por las empresas obligadas, y en concreto dentro de la información sobre cuestiones sociales y relativas al personal.

El alumbramiento del nuevo derecho a la desconexión digital en el ámbito laboral trae causa de la creciente hiperconectividad que permite hablar, aunque no es su única causa, de «la sociedad del cansancio»[17].

Los cambios en el «espacio» y, especialmente, en el «tiempo» del trabajo hacen emerger el riesgo de la «fatiga» informática a que hace referencia el artículo 88.3 de la Ley Orgánica 3/2018. Recuérdese que, para bien o para mal, la prevención de riesgos laborales es la base jurídica y el enfoque de la Directiva 2003/88/CEE, 4 noviembre 2003, del Parlamento Europeo y del Consejo, que regula determinados aspectos de la ordenación del tiempo de trabajo[18].

Además del respeto a los tiempos del descanso del trabajador ampliamente entendidos, se busca también conciliar la vida laboral con la personal y la familiar.

Aunque en la Ley Orgánica 3/2018, al contrario de lo que sucede con la legislación francesa, el protagonismo lo tiene la «política interna» elaborada por la empresa (artículo 88.3), lo cierto es que hay una mención expresa –y hasta una llamada, cabría decir– a la negociación colectiva o, en su defecto, al acuerdo entre la empresa y los representantes de los trabajadores (artículo 88.2), que se suma a la referencia más general que se hace a los «derechos digitales en la negociación colectiva» en el artículo 91 de la Ley Orgánica 3/2018, del que luego se dará cuenta. Existen ya experiencias y precedentes al respecto en la negociación colectiva española[19].

La legislación francesa fue pionera en el reconocimiento del derecho a la desconexión digital[20], estableciendo que, con efecto de 1 de enero de 2017, la negociación colectiva anual sobre igualdad profesional entre las mujeres y los hombres y la calidad de vida en el trabajo, tiene que incluir: (i) las modalidades del pleno ejercicio por el trabajador de su derecho a la desconexión; (ii) la puesta en marcha por la empresa de sistemas de regulación de la utilización de los dispositivos digitales, a fin de asegurar el respeto del tiempo de descanso y de vacaciones, así como de su vida personal y familiar. Solo en defecto de falta de acuerdo en la negociación, la ley francesa dispone que la empresa, previa audiencia de los representantes de los trabajadores, debe elaborar una «política de actuación» sobre las modalidades de ejercicio del derecho a la desconexión[21].

---

17. Byung-Chul Han, La sociedad del cansancio, Barcelona (Herder Ed.), 2017, 2ª ed. ampliada.
18. De gran utilidad es la «Comunicación interpretativa» de la Comisión Europea sobre esta Directiva (2017/C 165/01) publicada en el DOUE de 24 de mayo de 2017.
19. Véase, C. H. Preciado, *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, cit., pp. 147 y ss.. Monográficamente se remite a G. L. Barrios, «El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones», *Revista Aranzadi Doctrinal* núm. 1/2019, BIB 2018\14719, y a los autores allí citados.
20. Se trata del artículo 55 de la Ley nº 2016-1088 de 8 de agosto, que da nueva redacción al artículo 2242-8 del Code du Travail (JORF de 9 de agosto de 2016).
21. Remito a J. R. Mercader, El futuro del trabajo en la era de la digitalización y la robótica, cit., p. 162.

De forma más limitada, la Ley italiana de 22 de mayo de 2017 (n. 81) dispone que el acuerdo, por tiempo determinado e indeterminado, sobre la modalidad del trabajo «*agile*» (parte en la empresa y parte fuera de la empresa), debe establecer el tiempo de descanso del trabajador y las medidas técnicas y organizativas necesarias para asegurar «la desconexión del trabajador de los instrumentos tecnológicos de trabajo».

Por lo que se refiere a los antecedentes del artículo 88 de la Ley Orgánica 3/2018, no está de más recordar, de un lado, que el acuerdo de investidura PP-Ciudadanos de 2016 incluía, entre distintas medidas para «adaptar nuestro mercado de trabajo a la Cuarta Revolución Industrial», la de analizar «el reconocimiento del derecho a la desconexión» y, de otro, la proposición no de ley 162/000384 del Grupo Parlamentario Socialista[22] sobre protección de los derechos digitales de la ciudadanía. La proposición consistía en que el Congreso de los Diputados instaría al Gobierno a presentar un Proyecto de Ley para garantizar, entre otros, los «derechos de ciudadanía», entre los que se incluiría el «derecho a la desconexión laboral».

5.4. EL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO

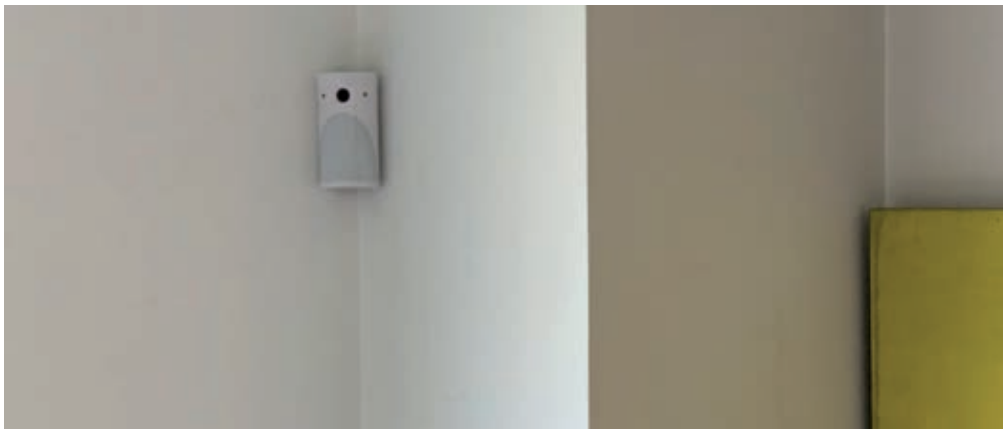
El artículo 89.1 de la Ley Orgánica 3/2018 establece que «los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores (o los empleados públicos) previstas, respectivamente, en el artículo 20.3 del ET (y en la legislación de función pública), siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Al artículo 89 de la Ley Orgánica 3/2018 remite el artículo 22.8 de esa Ley Orgánica. El artículo 22 de la Ley Orgánica 3/2018 se dedica al «tratamiento con fines de videovigilancia».

A destacar que se reconoce el derecho empresarial para ejercer el derecho de «control» del artículo 20.3 del ET, pero siempre que ello se haga «dentro de su marco legal y con los límites inherentes al mismo», lo que supone una implícita apelación a su definición internacional, supranacional, constitucional y legal y a su integración jurisprudencial igualmente internacional, supranacional, constitucional y del Tribunal Supremo.

Los empleadores han de «informar» de la medida de videovigilancia «con carácter previo, y de forma expresa, clara y concisa, a los trabajadores (o los empleados públicos) y, en su caso, a sus representantes».

De nuevo se manifiesta la importancia, absolutamente determinante, de la información a los trabajadores, explicitándose expresamente esta vez que la información ha de ser «previa», «expresa», «clara» y «concisa». Puede llamar la atención la utilización del término «concisa» por el artículo 89.1 de la Ley Orgánica 3/2018, frente al término «inequívoca» del artículo 90.2 de esa Ley Orgánica al que más adelante se hace referencia y más frecuente en el Reglamento (UE) 2016/679. Aunque no es seguro que sea así, puede que el término «concisa» traiga causa de la información «de carácter general» a que se refería la STEDH, 9 de enero de 2018 (López Ribalda I; recuérdese que esta sentencia ha sido revocada por la STEDH,

22. BOCG, Congreso de los Diputados, D Serie d núm. 139, 7 de abril de 2017.



Gran Sala, 17 de octubre de 2019, López Ribalda II; pero López Ribalda I se tuvo en cuenta en el debate de la Ley Orgánica 3/2018), así como con lo que se va a decir inmediatamente a continuación.

El párrafo segundo del artículo 89.1 de la Ley Orgánica 3/2018 dispone que «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores (o los empleados públicos) se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica»[23]. El artículo 22.4 de la Ley Orgánica 3/2018 establece que «el deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679». De momento, se trata del distintivo de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

Esta previsión se relaciona con el supuesto enjuiciado y con la doctrina sentada por la importante STC (Pleno) 39/2016, de 3 de marzo, con votos particulares, que rectifica la anterior STC 29/2013, de 11 de febrero, también con voto particular. A la STC 39/2016 se ha hecho ya referencia. La previsión tiene también en cuenta la STEDH, 9 de enero de 2018 (López Ribalda I), expresamente mencionada en algunas enmiendas presentadas al Proyecto de Ley Orgánica; recuérdese, no obstante, que la sentencia López Ribalda I ha sido revocada por la STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II).

La previsión se hace cargo, así, de que si se sospecha que se están cometiendo actos ilícitos y para descubrir a sus autores se implantan dispositivos de videovigilancia, una información previa muy detallada y pormenorizada puede frustrar el legítimo objetivo empresarial de identificar a esos autores[24].

---

23. El proyecto de Ley Orgánica hablaba inicialmente de comisión fragante de un acto «delictivo».
24. M. Falguera ha puesto de manifiesto las dificultades y consecuencias que el aviso previo tiene desde la perspectiva del derecho a la tutela judicial efectiva sin indefensión (artículo 24 de la CE) de la empresa («Nuevas tecnologías y trabajo (II): perspectiva constitucional», La Ley 6522/2016, pp. 20-21). Se facilita la existencia, así, hasta cierto punto, de controles «ocultos» (C. H. Preciado, *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, cit., p. 172 del original). Recuérdese que ya la conocida STC 186/2000, de 10 de julio, hacía referencia al hecho de que la instalación de un circuito cerrado de televisión no se pusiera en conocimiento de los trabaja-

Como se ha dicho gráficamente sobre los controles *ad hoc*, «el secreto del control es la garantía de su eficacia»[25]. Recuérdese, en este sentido que, como se ha anticipado, la importante STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II) señala que «si bien no cabe aceptar que la más mínima sospecha de que las irregularidades han sido perpetradas por los empleados pueden justificar una videovigilancia secreta (el subrayado es mío) por parte del empleador, la sospecha razonable de que se habían cometido graves irregularidades y el alcance de las mismas producidas en este caso pueden considerarse justificaciones serias, especialmente si, como ocurría en el caso, se sospechaba de la acción concertada de varios empleados».

Ha de tenerse en cuenta, en este sentido que, así como en prácticamente todas las empresas tendrán que establecerse criterios de utilización de los dispositivos digitales puestos a su disposición por su empleador (es difícil de imaginar en la actualidad una empresa en la que los empleados, o al menos parte de ellos, no usen dispositivos digitales), no en todas las empresas, ni muchos menos, existirán sistemas de videovigilancia, sino que estos se implantarán no pocas veces precisamente cuando exista alguna sospecha de comisión de actos ilícitos con vistas a la identificación de sus autores, teniendo en cuenta que la carga de la prueba recae íntegra y exclusivamente sobre la empresa (artículos 105.1 y 114.3 LRJS) y que esta es también titular del derecho fundamental a la tutela judicial efectiva sin indefensión y a utilizar los medios pertinentes para su defensa (artículo 24.1 y 2 CE).

Ya he dicho que creo que es un elemento relevante la existencia de sospechas, pues una cosa es un sistema de videovigilancia instalado con carácter permanente (y no ante la existencia de concretas sospechas) y otra un sistema de videovigilancia instalado *ad hoc* ante la existencia de sospechas, sistema que será en principio temporal y no permanente. Tras la Ley Orgánica 3/2018, en el primer caso habrá que proporcionar la información previa, expresa, clara y concisa que exige el párrafo primero del artículo 89.1 de la Ley Orgánica 3/2018, mientras que en el segundo valdrá el dispositivo al que se refiere el párrafo segundo del artículo 89.1 de la Ley Orgánica 3/2018 y al que se refería la STC 39/2016[26].

---

dores afectados «sin duda –era– por el justificado temor de la empresa de que el conocimiento del sistema de filmación frustraría la finalidad apetecida». En la misma línea, ya se ha dicho, y se volverá a reiterar enseguida, que la STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II) acepta, en determinados casos y condiciones, la videovigilancia «secreta».

25. A. y E. Desdentado, «La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador», cit.. Ya la STC 186/2000 se refería a la ausencia, por parte de la empresa, de información previa al trabajador con estas palabras: «sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida». En la misma línea, ya se ha dicho, y se volverá a reiterar enseguida, que la STEDH (Gran Sala) 17 de octubre de 2019 (López Ribalda II) acepta, en determinados casos y condiciones, la videovigilancia «secreta».

26. Aunque los hechos que enjuicia son anteriores a la entrada en vigor de la Ley Orgánica 3/2018, la sentencia del Juzgado de lo Social nº 3 de Pamplona 52/2019, de 18 de febrero, parece entender que –sin tampoco suscitar el debate de si habría que, en su caso, plantear cuestión prejudicial– no es válida la «excepción» del párrafo segundo del artículo 89.1 de la Ley Orgánica 3/2018. La sentencia lo justifica en que, a su juicio, así debe interpretarse tras la STEDH López Ribalda I (recuérdese que esta sentencia ha sido revocada por la STEDH, Gran Sala, 17 de octubre de 2019; López Ribalda II) y porque –asimismo entiende– el Reglamento UE 2016/679 no admitiría excepción alguna al cumplimiento de los deberes de información. Pero ha de recordarse que incluso la STEDH López Ribalda I, admitía expresamente que en el caso

Según se acaba de ver, el artículo 89.1 de la Ley Orgánica admite la grabación de imágenes en los términos expuestos, sin –podría pensarse– demasiadas restricciones, al menos expresamente formuladas, más allá de la mención al «marco legal» y a los «límites» a él «inherentes», mención sobre la que ya se ha reflexionado.

De conformidad con lo que expresa bien la importante y conocida STC 98/2000, de 10 de abril, distinto es el caso de la grabación de sonidos, contemplada mucho más restrictivamente que la grabación de imágenes por los apartados 2 y 3 del artículo 89 de la Ley Orgánica 3/2018.

En efecto y en primer lugar, el artículo 89.2 de la Ley Orgánica 3/2018 establece que «en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores (o los empleados públicos), tales como vestuarios, aseos, comedores y análogos». Hay que subrayar que esta prohibición comprende no solo la grabación de sonidos, sino también la videovigilancia. En el artículo 89 de la Ley Orgánica 3/2018, el concepto de videovigilancia parece ceñirse a la grabación de imágenes. La prohibición de videovigilancia, siquiera sea a efectos de seguridad y no del control del artículo 20.3 del ET y ni siquiera en los comedores y análogos (es plenamente entendible en los vestuarios y aseos), puede ser problemática. Cabe afirmar que es distinto, en este sentido, un vestuario o un aseo que un comedor o similar en donde quizás se pudiera permitir la videovigilancia en el acceso y salida.

En segundo lugar, más relevante es aún señalar que el artículo 89.3 de la Ley Orgánica 3/2018 dispone que «la utilización de sistemas similares a los referidos en los apartados anteriores (del artículo 89) para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores (del artículo 89)».

La grabación de sonidos en el lugar de trabajo solo es posible, por tanto, cuando sean relevantes los riesgos para la seguridad de las instalaciones, bienes y personas y siempre ha de respetarse el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores del artículo 89 de la Ley Orgánica 3/2018. Esta única mención del principio de proporcionalidad en el artículo 89.3 de la Ley Orgánica 3/2018, en el contexto de sus artículos 87 a 91, no puede interpretarse en el sentido de que las medidas empresariales previstas en otros preceptos y apartados de los artículos citados no estén igualmente sujetas a dicho principio de proporcionalidad, toda vez que sí lo están de conformidad con la jurisprudencia a la que se ha ido haciendo referencia, pues esa es la definición de «los derechos reconocidos constitucional y legalmente» (artículo 87.3 de la Ley Orgánica 3/2018), su «marco legal» y sus «límites inherentes» (artículo 89.1 de la Ley Orgánica 3/2018). Distinto puede ser el caso de la referencia al principio de la «intervención

---

se hubiera dado alguna información «incluso de carácter general», lo que no ocurrió en el supuesto. Sobre el Reglamento UE 2016/679, el Juzgado de lo Social se fi ja en sus artículos 12 a 14 y 88. Pero este último precepto no deja de hablar, no solo de normas «específicas» (que no necesariamente han de ser de mejora), sino también «adecuadas». Siendo los hechos asimismo anteriores a la Ley Orgánica 3/2018 (a la que no se menciona en ningún momento), un planteamiento contrario tiene la sentencia del Juzgado de lo Social nº 3 de Bilbao 128/2019, de 4 de abril: la sentencia declara válida la prueba videográfica.

mínima», que seguramente quiera expresar la diferencia entre la grabación de imágenes y la de sonidos, contemplada, como ya se ha dicho, necesariamente de forma más restrictiva.

En todo caso, «la supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley» (último inciso del artículo 89.3 de la Ley Orgánica 3/2018)[27].

5.5. LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL

El artículo 90 de la Ley Orgánica 3/2018 («derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral») establece, en su apartado 1, que «los empleadores podrán tratar los datos obtenidos a través de sistemas 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 ET (y en la legislación de función pública), siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo».

El artículo 90.1 de la Ley Orgánica 3/2018 reconoce, así, el derecho empresarial a implantar sistemas de geolocalización para ejercer las funciones de control del artículo 20.3 del ET, repitiéndose la llamada, que ya se hacía respecto de la videovigilancia en el artículo 89.1 de aquella Ley Orgánica, al «marco legal» y sus «límites inherentes». Se tiene por reproducido aquí lo que ya se dijo entonces.

27. «Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones» (primer inciso del párrafo primero del artículo 22.3 de la Ley Orgánica 3/2018).

Por su parte, el artículo 90.2 de la Ley Orgánica 3/2018 dispone que «con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores (o los empleados públicos) y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos», añadiéndose que «igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión».

Una vez más se pone de manifiesto la decisiva importancia de la información a los trabajadores, que ha de ser «previa», «expresa», «clara» e «inequívoca» sobre la existencia y características de los dispositivos.

El artículo 90.2 de la Ley Orgánica 3/2018 establece la obligación empresarial adicional de informar a los trabajadores del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión, lo que no se explicita de forma expresa en el caso de videovigilancia en el artículo 89.1 de la Ley Orgánica 3/2018.

Por el contrario, el artículo 90 de la Ley Orgánica 3/2018 no hace referencia al principio de proporcionalidad (artículo 89.3), –lo que, como ya se advirtió, no quiere decir que no se aplique–, ni tampoco a la comisión flagrante de un acto ilícito (artículo 89.1, párrafo segundo), cuando es también cierto que la geolocalización puede implantarse tras la existencia de sospechas de uso ilícito por el trabajador del vehículo y aunque es verdad que aquí no existe el dispositivo informativo del artículo 22.4 de la Ley Orgánica 3/2018 (ya se ha dicho que todavía hoy se trata del distintivo de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos)[28].

5.6. DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA

El artículo 91 de la Ley Orgánica 3/2018 («derechos digitales en la negociación colectiva») establece 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»[29].

El precepto adjudica «clásicamente» así a los derechos de la Ley Orgánica 3/2018 la naturaleza de derechos mínimos de manera que la negociación colectiva puede mejorarlos (establecer «garantías adicionales») pero no empeorarlos.

5.7. EL NUEVO ARTÍCULO 20 BIS DEL ET

La disposición final decimotercera de la Ley Orgánica 3/2018 añade un nuevo artículo 20 bis al ET[30] con el siguiente texto:

---

28. Sobre la geolocalización es de gran interés, aunque no era todavía aplicable la Ley Orgánica 3/2018, la sentencia de la Sala de lo Social de la Audiencia Nacional 13/2019, 9 de enero de 2019. La sentencia hace referencia al artículo 90.2 de la Ley Orgánica 3/2018.
29. Sobre «el papel de la negociación colectiva en la configuración de los derechos derivados de la Ley (3/2018)», remito a la nota con ese título de A. Baylos publicada en su *blog*.
30. Se remite a J. Mª Quílez, «La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores», *Revista Española de Derecho del Trabajo*, núm. 217, febrero 2019. El autor no se refiere solo al nuevo artículo 20 bis del ET, sino que aborda todo el

«Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».

5.8. OTRAS PREVISIONES DE LA LEY ORGÁNICA 3/2018, EN ESPECIAL LOS SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS[31]

El artículo 24 de la Ley Orgánica 3/2018 se ocupa de los «sistemas de denuncias internas», que se definen, en su apartado 1, como «sistemas de información» a través de los cuales puede «ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable»[32]. Pues bien, el artículo 24.1 de la Ley Orgánica 3/2018 parte de que es «lícita» la creación y mantenimiento de estos sistemas de información, de cuya «existencia» deben «ser informados» los «empleados y terceros».

El artículo 24.2 de la Ley Orgánica 3/2019 determina que el acceso a los datos contenidos en estos sistemas queda limitado exclusivamente a quienes desarrollan funciones de control interno y de cumplimiento o a los encargados del tratamiento, si bien «será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan». El precepto añade que el acceso se puede permitir al «personal con funciones de gestión y control de recursos humanos» solo «cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador».

Deben adoptarse «las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado» y «los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados» (artículo 24.3 y 4 de la Ley Orgánica 3/2019).

---

contenido laboral de la Ley Orgánica 3/2018.

31. Remito, con carácter general, a J. R. Mercader, «Aspectos laborales de la Ley Orgánica de Protección de Datos Personales, la garantía de los derechos digitales al margen», de próxima publicación, y que he podido consultar por la generosidad de su autor.
32. Sobre esta materia, remito con carácter general al trabajo de D. Martínez Saldaña e I. Moreno, «La protección del *whistleblower* y el *compliance* laboral», *Revista de Información Laboral*, 2018, núm. 12, pp. 83 y ss. El trabajo, centrado en la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión de 23 de abril de 2018 [COM (2018) 218 final. 2018/0106 (COD)], tiene ya en consideración el Proyecto de Ley que luego se convertiría, sin variar el texto, en la Ley Orgánica 3/2018. Ya se publicado en el DOUE la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, 23 octubre 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

Otros preceptos de la Ley Orgánica 3/2019 que merecen ser citados aquí son, en primer lugar, el artículo 5 que, en su apartado 1, establece que «todas las personas que intervengan en cualquier fase del tratamiento de datos» (por lo tanto, los trabajadores de la empresa que así lo hagan[33]) «estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679»; y, en su apartado 3, dispone que aquella obligación se mantiene «aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento».

En segundo lugar, su artículo 9 que menciona la «afiliación sindical» como una categoría «especial» de dato, de forma que «a los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar» esa afiliación sindical.

Podría suscitarse la cuestión de la compatibilidad del artículo 11.2 LOLS con el artículo 9 de la Ley Orgánica 3/2018, pero, si bien es claro que el precepto de la LOLS ha de cohonestarse desde luego con el de la Ley Orgánica 3/2018, no parece difícil encuadrar el supuesto del artículo 11.2 de la LOLS en el párrafo segundo del artículo 9.1 de la Ley Orgánica 3/2018 y, en particular, en las letras b) –a destacar la referencia que se hace al «convenio colectivo»– y d) del artículo 9.2 del Reglamento (UE) 2016/679. Como bien dice el Preámbulo de la Ley Orgánica 3/2018, «los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea»[34].

En tercer lugar, el artículo 19.1 de la Ley Orgánica 3/2019, de conformidad con el cual:

«Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios».

En cuarto lugar, el artículo 21 de la Ley Orgánica 3/2019 («Tratamientos relacionados con la realización de determinadas operaciones mercantiles»), de conformidad con el cual:

«1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

33. Desde esta perspectiva, es de interés el artículo de H. Monzón, «El deber de protección de datos personales de los trabajadores y su transgresión», *Revista de Información Laboral*, 2017, núm. 2.
34. El Preámbulo advierte que «la prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas».

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica».En quinto lugar, el artículo 36.2 de la Ley Orgánica 3/2019 («Posición del delegado de protección de datos»), de conformidad con el cual:

«Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses».

El artículo 36.2 de la Ley Orgánica 3/2019 se relaciona y desarrolla el artículo 38 del Reglamento (UE) 2016/679, cuyo apartados 3 y 5 disponen que se ha de garantizar que el delegado de protección de datos «no reciba ninguna instrucción en lo que respecta al desempeño de (sus) funciones», que aquel delegado «rendirá cuentas directamente al más alto nivel jerárquico» y, en fin, que el delegado está «obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones».

Finalmente, el artículo 22 de la Ley Orgánica 3/2019 sobre «tratamiento con fines de videovigilancia» a fin de «preservar la seguridad de las personas y bienes» (apartado 1) y a cuyos apartados 4 y 8 ya se hizo referencia en su momento.

La utilización de las nuevas tecnologías digitales genera grandes cantidades de datos relativos a las personas usuarias, cuyo conocimiento y tratamiento plantean riesgos evidentes para sus derechos y libertades, en concreto para sus derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la protección de datos personales y, por tanto, para los sistemas constitucionales democráticos en las sociedades digitalizadas, incluida nuestra Constitución, que reconoce y tutela esos derechos fundamentales.

Esta Monografía recoge los ensayos que, en el ciclo de conferencias organizado por la Fundación Ramón Areces sobre «El derecho a la protección de datos personales en la sociedad digital», se expusieron en la primavera y primeros día del verano de 2019 por cuatro destacados especialistas del tratamiento normativo de estos derechos: Juan Luis Requejo Pagés, José Luis Piñar Mañas, Mercedes Pérez Manzano e Ignacio García-Perrote Escartín. Sus aportaciones han desentrañado y valorado la adecuación de las garantías levantadas en defensa del derecho a la protección de datos personales por la Constitución, el Derecho de la Unión Europea, la Ley Orgánica 3/2018, de 5 de diciembre, el sistema jurídico penal y la legislación laboral.

FUNDACIÓN
RAMÓN ARECES

Vitruvio, 5 – 28006 Madrid
www.fundacionareces.es
www.fundacionareces.tv