ENCUESTA

ENCUESTA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

PRESENTACIÓN

En el momento en que redactamos esta presentación nuestras condiciones y patrones de vida son diferentes a como eran hace solo unos meses. La pandemia producida por el virus SARS-CoV-2 y las medidas adoptadas para hacerle frente, tanto a nivel institucional como personal, han producido una notable aceleración en todos los procesos de transformación de nuestra sociedad. Entre ellos destaca de forma especial la dependencia de las tecnologías de la información. Como consecuencia de la necesidad de mantener cierta distancia física entre nosotros y evitar los contactos que no sean imprescindibles, los medios tecnológicos nos han permitido desarrollar la actividad profesional a través del teletrabajo, realizar actividades comerciales, implementar un modelo de educación no presencial o semipresencial, e incluso mantener las relaciones sociales y familiares.

Pero esta nueva dependencia tecnológica plantea también no pocos retos a nuestra forma de organización política, la propia del Estado social y democrático de derecho, y a la garantía de los valores y derechos a los que responde ese modelo de organización. Por eso nos pareció oportuno que *Teoría y Realidad Constitucional* dedicase la encuesta que abre este número a la protección de datos personales; ello nos permitirá vislumbrar el alcance de esos retos a los que tendremos que enfrentarnos los constitucionalistas en los próximos años.

Quizás no sea exagerado decir que el precio que tienen que pagar los ciudadanos por el uso de la tecnología es el de permitir que terceros utilicen y traten sus datos personales. Podría parecer que este hecho no tiene excesiva trascendencia constitucional; sin embargo, esta circunstancia puede condicionar seriamente la libertad que necesitan las personas para actuar como ciudadanos libres y responsables en un Estado democrático de derecho y, con ello, el correcto funcionamiento de este tipo de Estados. Por eso, hace ya unas décadas los sistemas constitucionales reconocieron un derecho fundamental a la protección de datos personales, para garantizar la posición de esos ciudadanos frente a las amenazas y peligros de las nuevas tecnologías. En qué medida se ha conseguido este objetivo es algo que tendremos que valorar.

El derecho a la protección de datos personales tiene unas características específicas, como lo son también las amenazas a las que pretende hacer frente. Así, puesto

que el movimiento de datos es transnacional, este derecho se ha construido a partir de impulsos tanto nacionales como internacionales, destacando entre estos últimos los provenientes de las instituciones europeas. El resultado es un derecho que, al menos en el ámbito de la Unión Europea, tiene una configuración común en todos los Estados miembros y también un desarrollo normativo armonizado de su régimen jurídico. Podríamos decir pues que es un buen ejemplo de cómo se pueden construir elementos constitucionales comunes en el proceso de integración europea.

Desde otro punto de vista, estamos ante un derecho de especial complejidad, sobre todo porque se ejerce en un ámbito que tradicionalmente ha resultado ajeno a los constitucionalistas, que puede exigir ciertos conocimientos técnicos y que está en constante evolución. Esto significa, entre otras cosas, que en la medida en que los riesgos cambien, como resultado de los avances técnicos, también deberá evolucionar la regulación e interpretación de este derecho, pues de otro modo este podría terminar resultando ineficaz.

Abrimos pues el presente número con una encuesta en la que, como es norma habitual, un grupo de reconocidos especialistas en esta compleja materia nos ayudarán a entender la relevancia del derecho a la protección de datos personales y a valorar en qué medida ha logrado los objetivos que justificaron su reconocimiento, así como también a ser conscientes de la magnitud de los retos que tendremos que afrontar como consecuencia de la dependencia tecnológica que caracteriza ya a nuestra sociedad.

CUESTIONES

1. *El derecho fundamental a la protección de datos personales se reconoció en Europa en las últimas décadas del siglo* XX *con el fin de hacer frente a las amenazas que suponían los avances tecnológicos para la intimidad y la vida privada de las personas ¿Qué consideraciones quiere hacernos sobre dichas amenazas y sobre cómo han evolucionado hasta hoy en día?*

2. *¿Considera que el reconocimiento de un derecho fundamental es el medio más adecuado para hacerles frente? Desde una perspectiva más general ¿qué reflexiones cabe hacer sobre las posibilidades con las que cuentan el Estado y el Derecho para hacer frente a amenazas de ese tipo?*

3. *En el proceso de reconocimiento y determinación de este derecho fundamental han intervenido actores nacionales e internacionales. En este sentido ¿cree que el derecho a la protección de datos puede considerarse un ejemplo de derecho construido en un contexto de integración supranacional e incluso de globalización para hacer frente precisamente a una amenaza transnacional? ¿Qué balance haría de tal proceso?*

4. *¿Qué valoración le merecen las aportaciones jurisprudenciales que tanto a nivel nacional como internacional se han hecho a la construcción de este derecho? En concreto, ¿considera suficiente el amparo constitucional del derecho en España ofrecido por el artículo 18.4 de nuestra Carta Magna y el desarrollo que ha realizado el Tribunal Constitucional a partir del mismo?*

5. *La intervención del legislador en materia de protección de datos resulta imprescindible. ¿Cómo valora la regulación realizada tanto a nivel nacional como comunitario? Y en concreto ¿qué opina de su extensión, complejidad y accesibilidad para los ciudadanos? ¿Y desde el punto de vista de la justificación y previsión de límites al derecho?*

6. *En esta materia se han creado organismos independientes de garantía, como la Agencia Española de Protección de Datos ¿qué valoración le merece el régimen jurídico que se le ha dado? ¿Cree que sería necesaria o conveniente alguna modificación en su régimen jurídico o en algún otro aspecto del sistema de garantías de este derecho?*

ENCUESTADOS

LORENZO COTINO HUESO, Catedrático de Derecho Constitucional, Universidad de Valencia

ROSARIO GARCÍA MAHAMUT, Catedrática de Derecho Constitucional, Universidad Jaume I

PABLO LUCAS MURILLO DE LA CUEVA, Catedrático de Derecho Constitucional, Magistrado del Tribunal Supremo

MANUEL MEDINA GUERRERO, Catedrático de Derecho Constitucional, Universidad de Sevilla

ARTEMI RALLO LOMBARTE, Catedrático de Derecho Constitucional, Universidad Jaume I

LUCRECIO REBOLLO DELGADO, Catedrático de Derecho Constitucional, Universidad Nacional de Educación a Distancia

ANTONIO TRONCOSO REIGADA, Catedrático de Derecho Constitucional, Universidad de Cádiz

CAMINO VIDAL FUEYO, Profesora Titular de Derecho Constitucional, Universidad de Burgos

RESPUESTAS

1. *El derecho fundamental a la protección de datos personales se reconoció en Europa en las últimas décadas del siglo* XX *con el fin de hacer frente a las amenazas que suponían los avances tecnológicos para la intimidad y la vida privada de las personas ¿Qué consideraciones quiere hacernos sobre dichas amenazas y sobre cómo han evolucionado hasta hoy en día?*

LORENZO COTINO HUESO

El derecho de protección de datos a partir de la privacidad de la que hablara el juez Brandeis en 1890 ha ido haciendo frente a muy crecientes y cambiantes amenazas. El derecho a que le dejen a uno en paz («the right to be let alone»)

implicaba esencialmente una obligación esencial de abstención para terceros y poderes públicos, que otorgaba garantías frente a injerencias. Era, pues, una clásica libertad negativa del individuo. Sin embargo, esta visión puramente reaccional quedó muy insuficiente frente a unas tecnologías que han penetrado totalmente en la vida moderna con una afectación masiva y cotidiana a los derechos de la vida privada. Los importantes cambios tecnológicos han llevado a mutar este derecho, pasando a reconocer una capacidad de control a partir del consentimiento informado del interesado y toda una serie de derechos que, a su vez, implican fuertes deberes y obligaciones a quienes tratar datos personales. Asimismo, se han ido generando desde hace décadas instituciones especializadas para garantizar el cumplimiento de nuevos deberes.

Sin embargo, los riesgos e impactos generados por la informática no han parado de crecer exponencialmente con las nuevas tecnologías. La industria de la Web 2.0 o web social ha permitido interactuar a más de 4000 millones de personas generando extraordinarios datos de perfiles en manos de redes, grandes plataformas y tecnológicas. Sin embargo, ha sido la web 3.0 con la nube y el Internet de las cosas lo que ha incrementado las cantidades de datos, en una *segunda ola* de datos, como lo ha definido la UE en febrero de 2020. Más allá de las magnitudes de los datos acumulados, que se disparan, lo que supone la llamada industria 4.0 son las casi limitadas posibilidades de extraer información y que permiten generar valor añadido y patrones dinámicos de tendencias de futuro. Si hasta hace poco con los datos se podían hacer tantas cosas como las que cupieran en la imaginación humana, hoy día la explotación a través de sistemas de auto aprendizaje e inteligencia artificial permite extraer información y conocimiento a partir de los datos más allá de lo que puede previamente sospechar el ser humano.

Es por ello que la privacidad, la protección de datos y otros derechos fundamentales requieren de una actualización muy importante para preservar la dignidad humana y el libre desarrollo de la personalidad. Los nuevos tratamientos rehúyen del régimen jurídico de protección de datos o generan graves dificultades. Así, los datos fluyen mundialmente de manera aparentemente inubícua; muchas veces no son datos estructurados ni vinculables a personas concretas, por lo que no se aplicaría la protección de datos. El consentimiento informado y las finalidades determinadas para las que tratar los datos pasan a ser casi una entelequia frente a usos futuros que no se pueden prever. El principio esencial de la minimización de los datos a tratar pugna con los ingentes macrodatos. Asimismo, hoy día, más que tratamientos de datos especialmente sensibles, son especialmente preocupantes las finalidades de los tratamientos y perfilados que permiten las tecnologías disruptivas. Pese a que se traten datos no especialmente protegidos los impactos y riesgos requieren de especiales garantías.

Los datos son sin duda la materia prima esencial de la economía del siglo XIX. Sin embargo, la perspectiva de la protección de datos queda rebasada y de hecho se proclama una *soberanía digital* a la que hay que dar forma jurídica. Esta soberanía debe incluir, entre otras cosas, las facultades de propiedad o similares que

permitan monetizar a los sujetos su contribución a la economía digital con la materia prima de sus datos personales.

ROSARIO GARCÍA MAHAMUT

La evolución de la tecnología es de tal magnitud como exponenciales las ventajas que aporta y las amenazas que comporta más allá del tradicional conjunto de derechos fundamentales ligados a la privacidad. Por ello, de forma más práctica, quisiera acotar mis reflexiones al contexto actual en el que la lucha contra la pandemia de la Covid-19 nos ha lanzado del mundo presencial al mundo del ciberespacio afectando a todos los órdenes de la vida en un drástico confinamiento domiciliario repleto de dolor y desesperanza. La tecnología al servicio de la lucha contra la terrible crisis sanitaria se ha erigido en herramienta clave. Y el uso de la misma no ha afectado exclusivamente al flujo y tratamiento de los datos de salud (incluida la investigación científica) constreñido al ámbito sanitario; por el contrario, ha trascendido e impactado en todos los ámbitos de la vida de las personas y el de sus relaciones tanto en el entorno público como privado (ámbito laboral, educativo, económico, etc.).

En este contexto, hoy más que nunca, la exposición de nuestros datos personales en una realidad absolutamente digitalizada nos muestra con inusitada fuerza la doble cara de la moneda de una imparable tecnología que puede coadyuvar en algo tan decisivo como la lucha contra la pandemia a la vez que se puede convertir en la amenaza más contundente, no solo para la privacidad de las personas, sino para los principios y valores en los que se funda nuestro Estado.

Riesgos y amenazas *versus* oportunidades es la característica más definidora del avance tecnológico que parte del uso y de la sistematización de los datos personales. Avance tecnológico y amenazas constituyen realidades inescindibles. Solamente ciñéndonos a estos últimos meses recordemos los problemas que se han derivado de los usos y/o tratamientos de datos obtenidos a través de las distintas técnicas de reconocimiento facial cuando, por ejemplo, se determinó la migración de todas las actividades docentes en entornos online, geolocalizaciones en redes sociales, cámara de infrarrojos, apps de seguimiento, toma de temperatura indiscriminada sin anonimizar y sin supervisión de las autoridades sanitarias, usos de drones, etc., etc., etc. Todo ello acompañado de las oportunas brechas de seguridad mientras el flujo y transferencias de datos circulan allende de cualquier frontera física.

Resulta difícil poner en duda que la tecnología y los datos digitales, como bien ha puesto de relieve la Comisión Europea, tienen una valiosísima función que desempeñar en la lucha sanitaria contra la pandemia. Pero incluso en tal situación, como ha subrayado el Comité Europeo de Protección de Datos, «los principios generales de eficacia, necesidad y proporcionalidad deben dirigir cualquier medida adoptada por los Estados miembros o las instituciones de la UE que

implique el tratamiento de datos personales para combatir la Covid-19» (Directrices 04/2020, de 21 de abril). Por ello, no puedo estar más de acuerdo con la llamada a la cautela sobre el carácter irreversible de ciertas medidas que, en todo caso, deben ser necesarias, limitadas en el tiempo y de alcance mínimo. De ahí que también haga mía la afirmación del CEPD de que «nadie debe verse obligado a elegir entre una respuesta eficaz a la crisis y la protección de nuestros derechos fundamentales» porque, efectivamente, «la legislación europea en materia de protección de datos permite el uso responsable de datos personales para fines de gestión sanitaria, al tiempo que garantiza que en ese proceso no se erosionen los derechos y libertades individuales» (Directrices 04/2020, de 21 de abril).

Sin la menor duda, también en situación de emergencia sanitaria, el tratamiento de datos personales debe realizarse conforme al Reglamento General de Protección de Datos 2016/679 (RGPD) y a la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPDGDD) y, en consecuencia, deben ser tratados con licitud, lealtad, transparencia, limitación de la finalidad, exactitud y minimización de los datos. El principio de transparencia hoy más que nunca cobra un valor inusitado, como absolutamente relevante ha devenido la tecnología que puede contribuir a la lucha contra la Covid-19. Tecnología que, en modo, alguno puede dar la espalda a los principios generales de eficacia, necesidad y proporcionalidad.

PABLO LUCAS MURILLO DE LA CUEVA

En realidad, más que en las últimas décadas del siglo XX, el reconocimiento como derecho fundamental se produjo el año 2000. Se lo dio la Carta de los Derechos Fundamentales de la Unión Europea, que le dedicó su artículo 8. Ese mismo año el Tribunal Europeo de Derechos Humanos, en sus sentencias Amann y Rotaru, incluyó la protección de los datos personales entre los elementos garantizados por el artículo 8 del Convenio Europeo de Derechos Humanos. Y en España fue la sentencia del Tribunal Constitucional n.º 292/2000, de 30 de noviembre, la que dio el paso. Antes, desde mediados de los años sesenta se había ido avanzando en diversas regulaciones, primero para el ámbito público, luego, ya en los años setenta, también para el privado, que limitaban el acceso a los datos personales y su conservación y utilización. El Convenio n.º 108, de 28 de enero de 1981, del Consejo de Europa supuso un paso decisivo pues sentó los principios, plenamente válidos hoy en día, que debían observarse en el tratamiento automatizado de los datos personales. Pero esas regulaciones y principios carecían de un sustento claro, pues no se lo podían ofrecer ni el derecho a la intimidad ni el más amplio derecho a la vida privada. El problema venía y viene, principalmente, del acceso incontrolado a información personal que no se manifiesta en esas esferas de la intimidad o de la vida privada y de su tratamiento y utilización igualmente incontrolados.

Las capacidades para lo uno y para lo otro han aumentado exponencialmente de la mano del progreso tecnológico.

Por eso, si inicialmente se temía, en particular, que el Estado, el poder político, supiera todo de nosotros, creo que después se ha percibido que los problemas más importantes, al menos los que afectan a nuestra vida cotidiana, provienen tanto o más de los operadores privados y, en especial, aunque no exclusivamente, de las grandes corporaciones, sobre todo de las que dominan las tecnologías de la información y de las comunicaciones. Esta impresión ha ido aumentando al mismo ritmo en que se ha ido produciendo la migración de múltiples relaciones intersubjetivas al ciberespacio y nos vamos acercando a un escenario en el que la regla sea el trato telemático y la excepción el contacto personal. En ese contexto, las amenazas han crecido en progresión geométrica.

Las más recientes son las debidas a la vigilancia masiva de las telecomunicaciones que practican algunos Estados y a la tergiversación organizada de la realidad que se difunde, sobre todo, en el mundo de las redes sociales a veces, también, por obra de algunos Estados pero no de manera exclusiva.

MANUEL MEDINA GUERRERO

Es indudable que la Inteligencia Artificial (IA) y otras tecnologías digitales emergentes, como el Internet de las cosas, tienen un enorme potencial para promover el desarrollo económico y mejorar el estado de la sociedad en su conjunto. No es de extrañar, por tanto, que la IA constituya una prioridad en la agenda de la UE, con la que se pretende aprovechar al máximo los beneficios que el uso de los datos puede suponer para incrementar la productividad y la competitividad de los mercados (en esta línea, la agenda sobre el *Mercado Único Digita*l), así como para mejorar la prestación de los servicios públicos.

Pero no es menos evidente que el potencial que supone la utilización de sistemas de toma de decisiones automatizadas basadas en algoritmos conlleva también nuevos riesgos y amenazas para la privacidad: al fin y al cabo, con las decisiones automatizadas el individuo puede convertirse en un mero objeto de los programas informáticos. A este riesgo genérico a la *cosificación* del ser humano cabría añadir otros problemas que en la práctica pueden mostrar los sistemas algorítmicos, señaladamente que, bajo la pátina de una exquisita imparcialidad, se oculten en ocasiones determinados sesgos ideológicos.

El RGPD ofrece, sin embargo, una base jurídica que, rectamente interpretada, puede ser suficiente para conjurar buena parte de estos riesgos. En efecto, el RGPD parte de la regla general de que todo afectado tiene «*derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*» (art. 22.1). Y si bien es cierto que el segundo apartado del art. 22 excluye la aplicación del apartado primero en relación con determinadas decisiones, en

cualquier caso se asegura «*como mínimo el derecho a obtener intervención humana por parte del responsable*» respecto de algunas de tales decisiones (art. 22.3). El núcleo central de la garantía reside, por tanto, en que la decisión basada o apoyada en un programa informático esté siempre sometida a la supervisión de un ser humano, de tal modo que la responsabilidad sobre las decisiones que nos afectan no se pueda imputar exclusivamente a sistemas informáticos anónimos. Naturalmente, la eficacia real de esta garantía pasa por que la intervención humana sea sustantiva, no meramente formal.

Y dado que las decisiones automatizadas resultan especialmente intrusivas en la esfera de la privacidad cuando se trata de datos sensibles, dispone el art. 22.4 RGPD que las mismas «*no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1*», salvo que medie un consentimiento explícito del afectado o concurra un interés público esencial [art. 9.2 a) y g)] «*y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado*». Para aquilatar adecuadamente el calado de esta cláusula de garantía es preciso atender al Considerando 71, que pone el acento en que dichas medidas deben impedir*«entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religiosas o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto».*

Este mandato de no discriminación con base en datos sensibles que se deriva de la lectura conjunta del Considerando 71 y del art. 22.4 RGPD es susceptible de ser interpretado, al menos, bajo dos perspectivas. Desde una aproximación más restrictiva de su alcance, que probablemente erosionaría de modo sustancial su eficacia, sólo se aplicaría a aquellos casos en que un algoritmo utiliza directamente variables que se refieren de forma explícita a alguna de las categorías de datos mencionados en el artículo 9.1 RGPD. O bien puede partirse de una lectura más amplia de esta garantía, según la cual la misma brindaría también protección a aquellos supuestos en que, pese a no emplearse variables que identifiquen expresamente a los datos sensibles, utiliza sin embargo otras que están directa y estrechamente relacionadas con ellos.

Conviene por otro lado señalar que los riesgos que entrañan las nuevas tecnologías se proyectan con especial intensidad en relación con los menores, pues ya a partir de los catorce años pueden prestar su consentimiento respecto de los «*servicios de la sociedad de la información*» (art. 7 de la LO 3/2018 en conexión con el art. 8 RGPD). Y lo cierto es que el RGPD tampoco ha descuidado subrayar la protección específica que debe brindarse *«a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño»* (Considerando 38). Y aunque la regulación contenida en el art. 22 RGPD no aborda específicamente el tratamiento de datos relativo a los menores, el Considerando 71 parte de la tesis de que las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, no se debe aplicar a los

niños: «*{…} Tal medida no debe afectar a un menor*». ¿Qué alcance jurídico cabe atribuir a esta referencia del Considerando? El Grupo de Trabajo sobre protección de Datos del art. 29, en sus *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* (WP251rev.01), de 3 de octubre de 2017 —revisada el 6 de febrero de 2018—, sostiene que, al no estar reflejada en el propio artículo, no constituye «una prohibición absoluta de este tipo de tratamiento en relación con los niños». Y prosigue: «No obstante —prosiguen las *Directrices*—, teniendo en cuenta este considerando, el GT29 recomienda que, por lo general, los responsables del tratamiento no se basen en las excepciones del artículo 22, apartado 2 para justificarlo».

El incremento de la transparencia acerca de los algoritmos utilizados puede contribuir sin duda a reforzar la tutela de la privacidad. En este sentido, cabe señalar que el RGPD incluye entre la información que debe facilitarse a los afectados, tanto cuando se haya obtenido de los mismos como si no, la siguiente: «*la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*» [art. 13.2 f) y art. 14.2 g), respectivamente]. Si este deber de información llega tan lejos como para concluir que el responsable deba abrir también los algoritmos en que se fundamente la decisión, es una cuestión ciertamente controvertida. En línea de principio, cuando se trata de empresas e industrias tecnológicas, la apertura del contenido de sus logaritmos puede afectar negativamente a «*los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos*» (Considerando 63).

Diferente puede ser la valoración respecto de los algoritmos desarrollados por las Administraciones públicas en el desempeño de sus funciones. Pues en este supuesto entraría también en juego el derecho de acceso a la información pública consagrado en la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno; y, ciertamente, resultaría cuando menos llamativo que se considerase aplicable a logaritmos sufragados con fondos públicos el límite de la «*propiedad intelectual e industrial*» previsto en el art. 14.1.j) de esta Ley 19/2013.

Comoquiera que sea, pese al evidente avance que ha supuesto el RGPD para paliar las amenazas que entraña la toma de decisiones automatizadas, no puede dejar de señalarse que aún queda un margen de mejora en este ámbito, como ha puesto de manifiesto el Parlamento Europeo en su Resolución, de 12 de febrero de 2020, sobre *Procesos automatizados de toma de decisiones: garantizar la protección de los consumidores y la libre circulación de bienes y servicios*, en donde parece insinuarse una invitación a la Comisión para revisar la normativa existente en materia de consumo a fin de mejorar la tutela en este ámbito.

Los riesgos que las nuevas tecnologías suponen para la privacidad se exacerban cuando los prestadores de bienes o servicios online ostentan una posición dominante en el mercado, hasta el extremo de llegar a erosionar sustancialmente la capacidad de disposición que tienen los usuarios sobre sus propios datos. A este

respecto, las autoridades de control de la competencia pueden jugar un importante papel para mitigar las perniciosas consecuencias que conlleva para la privacidad la asimétrica posición de debilidad que tienen los ciudadanos frente a esas grandes empresas. Así lo pone de manifiesto la experiencia alemana: mediante decisión fechada el 6 de febrero de 2019, el *Bundeskartellamt* consideró contraria al derecho de la competencia la práctica de Facebook de condicionar la prestación del servicio a la adscripción por parte de los usuarios a otros servicios subsidiarios de la compañía y a sitios web de terceros. Aunque obviamente la decisión se fundamentó en la aplicación de la normativa antitrust al estimar que Facebook abusó de su posición dominante como red social en Alemania, fue determinante en su resolución la apreciación de que se había quebrantado el RGPD, habida cuenta de que no podía considerarse que los usuarios dieran su consentimiento libremente —tal y como exige su artículo 7.4— al existir «*un desequilibrio claro entre el interesado y el responsible del tratamiento*» (Considerando 43). La ratificación de esta decisión por el *Bundesgerichtshof* (Sentencia de 23 de junio de 2020) sienta las bases para una fructífera cooperación en este ámbito entre las autoridades de control de la competencia y las autoridades de supervisión de la protección de datos de los países miembros de la UE.

En lo concerniente a la centralidad que ostentan determinadas redes sociales, no puede dejar se apuntarse que las amenazas transcienden la esfera de la privacidad de los ciudadanos para llegar a afectar al mismo sistema político. Efectivamente, las plataformas digitales, en principio potencialmente llamadas a incrementar la participación ciudadana y por ende a reforzar la democracia, pueden operar como un factor desestabilizador de dicho sistema al facilitar que se influya en el momento electoral, arrostrándose así el riesgo de generar una «democracia hackeada», por utilizar la expresión de Martin Moore. La contundente Resolución del Parlamento europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de datos (2018/2855 (RSP)), ya advierte de las dimensiones de este desafío: sugiere que «*debe prohibirse la elaboración de perfiles para fines políticos y electorales, y la elaboración de perfiles sobre la base de comportamientos en línea que puedan revelar preferencias políticas*»; y «*pide a los partidos políticos y a otros actores que participen en las elecciones que se abstengan de utilizar perfiles para fines políticos y electorales*» (9).

El hecho de que «*las opiniones políticas*» constituyan una categoría especial de datos personales (art. 9.1 RGPD) facilita sin duda que se pueda articular un *test* estricto en torno a la licitud de su tratamiento incluso por parte de los propios partidos políticos (STC 76/2019).

Finalmente, aunque el listado de los riesgos tecnológicos podría extenderse más largamente, no podemos dejar de reseñar la amenaza para la privacidad que supone el empleo de técnicas de reconocimiento facial, cada vez más extendidas en diversos ámbitos pero especialmente en materia de prevención de delitos. La adecuada conciliación de los intereses en liza pasa por la aplicación de un test

riguroso sobre la proporcionalidad del tratamiento de estos datos biométricos (en esta línea, la Sentencia del Tribunal de Apelación, de 3 de septiembre de 2020, en la que se enjuició el sistema de reconocimiento facial empleado por la policía de Gales del Sur, [2020] EWCA Civ 1058).

ARTEMI RALLO LOMBARTE

La sociedad ha protagonizado transformaciones extraordinarias a lo largo de las últimas décadas y los enormes cambios sociales, económicos, institucionales o culturales ya no tienen una dimensión nacional sino global. Como hemos expuesto en un reciente trabajo («De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)», *Revista de Derecho Político*, 100, 2017, pp. 637-667), esta impredecible revolución tecnológica ha modificado pautas de comportamiento y relaciones humanas y el Derecho ha intentado ordenar esta revolución tecnológica regulando las nuevas conductas vinculadas al cambio tecnológico. La «informática» de la Constitución de 1978 evidenciaba la incipiente y primaria computerización pero hoy vivimos en plena sociedad de la información y del conocimiento y nos adentramos en los terrenos inexplorados e inciertos de la inteligencia artificial. En la era del *Big Data* y de la inteligencia artificial, los riesgos y amenazas a la protección de datos exigen un enfoque complementario a los mecanismos represores o sancionadores basado en una estrategia preventiva sustentada en los siguientes técnicas y principios: *accountability principle*, *privacy by design and by default*, *data minimization principle*, *privacy impact assessments*, *delegados de protección de datos* y *certificaciones y sellos*.

Obviamente, los poderes públicos no han permanecido ajenos a las necesarias modificaciones normativas que debían acompañar los cambios tecnológicos. Del origen, evolución y adaptación del derecho de protección de datos a esta realidad cambiante dan buena cuenta cuatro estadios normativos europeos perfectamente identificables: el Convenio 108 del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de sus datos personales; la Directiva 95/46/CE 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 art. 8 de la Carta de Derechos Fundamentales de la Unión Europea al que el Tratado de Lisboa otorgó fuerza jurídica a partir de 2009; el Reglamento General de Protección de Datos de 2016. Tres leyes nacionales (LORTAD, LOPD y LOPDGDD) han desarrollado los compromisos europeos adquiridos por España.

La Directiva 95/46/CE fue, sin duda, el gran aldabonazo y marcó la historia de éxito de la protección de los datos personales en Europa e, incluso, a nivel planetario. Pero, apenas dos décadas después, la vertiginosa evolución tecnológica y la globalización ofrecían *nuevos retos*: redes sociales con miles de millones de miembros en todo el mundo; la computación en nube con recursos compartidos en servidores remotos; la geolocalización que facilita la ubicación del individuo a

través de su dispositivo móvil; el necesario reforzamiento del mercado interior europeo de la protección de datos; las exigencias de las transferencias internacionales de datos; la plena efectividad de las normas sobre protección de datos; o la necesaria coherencia del marco jurídico europeo regulador de la protección de datos. La respuesta europea a estos retos vino de la mano del RGPD 2016/679 con vocación de superar la fragmentación europea de la protección de datos en aras de una mayor seguridad jurídica. El RGPD ha sido y es el instrumento jurídico idóneo para garantizar armonización y coherencia de la normativa europea de protección de datos a través de un régimen sancionador común: la previa *doble velocidad europea* en protección de datos, marcada en demasiadas ocasiones por la impunidad, ha dado paso a un RGPD que generaliza en todo el territorio de la Unión Europea un régimen de sanciones efectivas, proporcionadas y disuasorias. El RGPD afronta el tsunami tecnológico incrementando la transparencia e información al ciudadano, mejorando los procesos de otorgamiento del consentimiento, proporcionando especial protección a los menores, adicionando nuevos derechos como el derecho al olvido o a la portabilidad o perfeccionando los instrumentos de reacción social o jurisdiccional frente a vulneraciones masivas protagonizadas por los grandes servicios online. Además, el RGPD tiene la ambición de regir y resultar aplicable a entidades no establecidas en la Unión Europea, con sede en terceros países (particularmente, USA), lo que constituye un indiscutible avance en el sistema de garantías del derecho a la protección de datos en la era digital.

Todo ello evidencia que el marco normativo vigente goza de perfecta salud para afrontar los riesgos y amenazas que acechan la privacidad de la sociedad contemporánea. La sociedad está cambiando a un ritmo vertiginoso y es difícil pronosticar cuales de esos cambios afectarán especialmente al derecho de protección de datos. La imparable, generalizada y omnipresente digitalización —especialmente articulada en torno a los servicios de Internet— abre un proceso acumulativo de interrogantes sobre un derecho como el de protección de datos que nació y ha evolucionado, precisamente, al socaire de la progresiva digitalización. La digitalización total de nuestra sociedad, como resulta no solo intuible sino perfectamente perceptible en la actualidad, extiende la problemática de la protección de datos a todo ámbito imaginable: trabajo, ocio, salud, educación, etc. Si hubiera que identificar manifestaciones concretas de los desafíos que afronta la garantía efectiva del derecho a la protección de datos me atrevería a apuntar los siguientes: 1.º) con la generalizada banalización de la trasmisión de imágenes personales en cualesquiera espacios y redes, el reconocimiento facial se ha convertido en una muy peligrosa herramienta digital de alcance insospechado tanto en el ámbito público como privado; 2.º) la geolocalización adquiere un especial impacto vinculado al generalizado uso individualizado de dispositivos digitales que identifican a los usuarios en cualesquiera ámbitos; 3.º) la inseguridad digital convierte al ciudadano en un ser especialmente vulnerable no solo en su privacidad si no en cualesquiera otros aspectos: económicos, sociales, humanos.

LUCRECIO REBOLLO DELGADO

El conocimiento que el Estado ha tenido históricamente del ciudadano es sumamente escaso hasta la Revolución Francesa de 1798. Suele concretarse en aspectos tributarios o de prestación de determinados servicios, con un ámbito muy localizado y con una escasa capacidad de difusión e intercambio, y en definitiva de tratamiento. Era mayor el acopio de datos de la Iglesia, que llevaba un registro de sus fieles, a partir de la inscripción de su bautismo, matrimonio, defunción, entre los aspectos más importantes. Tampoco es de tener en cuenta, en estas épocas, la capacidad de intromisión del propio ciudadano en la íntima parcela de otro cualquier ciudadano. Es el Estado, fundamentalmente por la necesidad estadística, quien primero va a suscitar la problemática del acopio de datos, pero esta circunstancia no se producirá hasta la segunda mitad del s. XX.

En 1935 el presidente norteamericano Roosevelt aprueba la *Social Security Act*, que, con una finalidad social, pretendía la actualización de datos relativos a trabajadores como el derecho a la asistencia médica, pensiones y otros beneficios. Ello supuso el primer gran reto del tratamiento de datos por parte del Estado, debido al ingente número de éstos que se recogían, lo que había de multiplicarse por millones de trabajadores. Pero los medios técnicos de la época eran escasos, lo que supuso un cumplimiento parcial de los objetivos, a la vez que evidenció la necesidad de herramientas técnicas más evolucionadas para tan ingentes trabajos. Pero como es lógico deducir, las necesidades sociales en el ámbito civil o las pretensiones de las empresas no eran suficientes para dar el empuje necesario. A lo más que se había llegado era al descubrimiento del profesor alemán Konrad Suze en 1941, del denominado *Z3,* que apuntaba las posibilidades, a la vez que explicitaba las necesidades de mejoras del tratamiento de datos.

El verdadero impulso técnico viene de la pretensión constante, y de una no menor aportación económica, de mejorar y perfeccionar las técnicas de guerra. En 1943 un conjunto de expertos al servicio del ejército británico construyó el denominado *Colossus,* que tenía como finalidad descifrar en pocos segundos los mensajes secretos de los enemigos durante la II Guerra Mundial. También con motivo de la carrera armamentística, en 1945 se fabrica en Estados Unidos el ENIAC (*Electronic numerical integrator and calculator*) y se hace en el laboratorio de Los Álamos, donde se estaba desarrollando la bomba atómica. En el mismo año, el profesor John von Neumann formula lo que se considera como el primer programa de ordenador, que podía realizar una simple operación contable, pero ya establece las bases teóricas de los ordenadores.

En junio de 1950 se introducen las primeras aplicaciones civiles de la informática, la multinacional norteamericana Remington Rand entrega el primer ordenador de uso comercial, se fabrica ya en serie. Pero no está generalizado en el uso de la población, por lo que tenía una incidencia muy parcial

Pese a lo manifestado, tecnológicamente aún estaba por llegar lo mejor, la comunicación entre ordenadores. En 1965 L. Roberts y T. Merril conectan por

primera vez dos ordenadores a través de una línea de teléfono y constatan la facilidad con que pueden transmitirse datos de uno a otro, nace así ARPANET, que ya en 1970, además de los usos militares, ofrecía correo electrónico y transferencia de ficheros dentro de Estados Unidos, y en 1973 se conseguían las primeras conexiones internacionales.

El 1 de enero de 1983 se sustituye el protocolo NCP por el de TCP/IP, se separa la parte militar, denominada Milnet y surge INTERNET, que coexiste con ARPANET hasta 1990 y un año después apareció la World Wide Web como hoy la conocemos. La generalización de su uso alejaba la informática del ámbito técnico y la colocaba en la centralidad de la vida del ciudadano, ya no es únicamente una herramienta de trabajo, sino también un potentísimo medio global de intercambio de información de datos y un medio de comunicación social.

Pero pese a ser esta nueva tecnología un ejemplo de colaboración y solidaridad, así como una magnifica herramienta para la sociedad, pronto se confirmó que las potencialidades técnicas puestas en la mano del hombre corren el riesgo de lesionar derechos fundamentales, lo que requiere la intervención del Estado, para que, a través de la legislación, establezca medios para evitar la vulneración de derechos. El problema añadido ahora, con la generalización o globalización del uso de la Red, es que el Estado no tiene posibilidad efectiva de controlar determinadas actividades, su actuación se ve limitada por el ámbito de vigencia de las propias normas estatales. Como puede comprobarse, todo avance tecnológico, que implique un uso social, finaliza requiriendo la intervención jurídica, pero en este caso ya no únicamente del Estado, debido a que la existencia de un espacio virtual transfronterizo requiere para la informática y uso de la Red una regulación universal, que como veremos más adelante plantea no pocas dificultades.

Probablemente el primer autor consciente de este potencial peligro será Arthur R. Miller, quien ya en 1969 es consciente de los problemas jurídicos relacionados con la intimidad que puede generar la informática. También en 1972, A. Westin publicará una monografía con la misma preocupación, después de realizar un estudio de las bases de datos más importantes en Estados Unidos, y concluye su obra alertando sobre posibles usos lesivos.

Este interés por el uso lesivo de la tecnología se irá incrementando en la medida en que se producen mayores y mejores avances, y especialmente cuando se empieza a generalizar el uso del ordenador, no sólo por empresas o instituciones, sino también por particulares. De esta forma se inicia la regulación jurídica como la más plausible constatación del peligro respecto de derechos fundamentales que aquélla lleva implícita. Al contrario de lo que hubiera parecido lógico, es decir, que la primera norma sobre protección de datos surgiera en Estados Unidos, debido a que este país es pionero en el desarrollo de las tecnologías, su generalización y la multiplicidad de aplicaciones prácticas, será en Europa y de forma más concreta en el Land alemán de Hesse, donde se publicará la primera norma que limite el uso de la informática, se trata de la *Datenschutz,* de 7 de octubre de 1970, y le seguirá la Data Lag de Suecia en 1973.

Las nuevas tecnologías, al posibilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas y de recopilación de datos, se presentan como una amenaza ante el ciudadano, ya que el uso de los modernos medios electrónicos, estén en manos de quien estén, contraen el riesgo de vulnerar derechos. Pese a ello, no podemos establecer como única visión de los modernos medios de tecnología sólo la negativa. También y sin duda ofrecen un aspecto sumamente positivo en la actividad del ser humano, racionalizando y suprimiendo laboriosos trabajos, y sobre todo rompiendo, tanto en el ámbito laboral como social, las barreras del espacio y el tiempo.

Los datos y su facilidad de tratamiento constituyen indefectiblemente poder, y no cabe duda de que al Estado le es necesaria determinada información para cumplir sus fines. Pero no es menos cierto que un uso abusivo o incontrolado de los datos puede minar el funcionamiento de cualquier Estado. El mismo riesgo de acumulación de datos, al que está sometido el individuo por la acción del Estado, se reproduce por la acumulación de datos y la facilidad de tratamiento, por parte de otros ciudadanos.

Partiendo del principio democrático de que todo poder ha de estar necesariamente sometido al Derecho, es fácil deducir una solución incontestable, es decir, sometamos a la norma la actividad susceptible de lesionar derechos, tanto si la realiza el Estado, como si lo hacen los particulares. Esta solución está exenta de toda problemática o complejidad jurídica. Ahora bien, los problemas surgen en su aplicación práctica, en el desarrollo efectivo de tales medidas.

ANTONIO TRONCOSO REIGADA

La Constitución Española de 1978 señaló en el art. 18.4 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 los derechos». Los constituyentes fueron ya conscientes de que los avances tecnológicos, que deben estar siempre al servicio de la persona, pueden suponer también una importante amenaza para sus derechos. La primera etapa de desarrollo de la informática dominada por los grandes ordenadores —la de la macro-informática—, que ofrecían unas posibilidades de captar, relacionar, transmitir y acumular información personal prácticamente ilimitadas, daba paso a una segunda etapa caracterizada por la extensión de los ordenadores personales —la de la micro-informática—. Como ya recogía con acierto la Exposición de Motivos de la LORTAD, la informática, con su capacidad para almacenar datos y superar las barreras que en el pasado representaban el tiempo y el espacio —junto con las ya existentes técnicas de comunicación—, ofrecía un conjunto muy extenso de datos que configuraban un retrato de la persona y suponían una amenaza antes desconocida para la privacidad y para el ejercicio de otros derechos. En la primera etapa de la informática los riesgos eran principalmente los

grandes ficheros de las Administraciones Públicas y sus consecuencias se encuentran bien descritas en la Sentencia del Tribunal Constitucional Federal Alemán, de 15 de diciembre de 1983, que declaró inconstitucionales algunos preceptos de la Ley del Censo, de 4 de marzo de 1982: «Cualquiera que no esté seguro de si el comportamiento desviado se anota en cualquier momento y se almacena, utiliza o transmite permanentemente como información, tratará —de acuerdo con el principio del Panoptismo— de no llamar la atención con ese comportamiento». Esto no sólo perjudica las posibilidades del individuo de desarrollo y ejercicio de la libertad, sino también el bien común, porque la autodeterminación es una «condición funcional elemental de un sistema de gobierno democrático libre que está basado en la capacidad de actuar y de participar de sus ciudadanos» —BVerfGE 65, 1; Badura; Lucas Murillo—.

Con posterioridad estas amenazas no sólo han evolucionado sino que han crecido de manera exponencial con las llamadas —en ese momento— *nuevas* tecnologías de la información y la comunicación, sobre todo con la rapidez y la universalización de Internet a mediados de los años noventa del siglo pasado, que permitió la efectividad de los buscadores —*Yahoo* aparece en 1995—, las redes sociales —*LinkedIn* y *My Space* surgen en 2003—, la computación en la nube —2006—, el *Big Data* —2006—, el Internet de las cosas —2008—, la inteligencia artificial, el *Blockchain* —que nace en el 2008 de la mano del *Bitcoin* o mejor al revés—, el *Machine Learning*, etc. En general, las fechas de comienzo de las tecnologías son muy difusas, aunque hay excepciones, existiendo una gran distancia temporal entre las primeras definiciones teóricas, los primeros desarrollos y la implantación de un producto en el mercado. El término *Big Data*, que hace referencia al análisis de grandes volúmenes de información de fuentes heterogéneas no estructuradas y a gran velocidad, se empieza a usar en los años 90 del siglo pasado, aunque es en 2006 cuando se populariza de la mano de *Google*, si bien había estudios, prototipos y quizás alguna *startup* antes. El *cloud*, aunque se difunde en la primera década del siglo XXI, empieza a pergeñarse ya a finales de los años 80, apareciendo en 1995-96 las primeras empresas de esa tecnología. En 1956 se celebra el primer *workshop* universitario sobre inteligencia artificial; comienza a investigarse esta cuestión en el decenio de 1960, pero no es hasta finales de los años 80 o principios de los 90 cuando adquiere carta de naturaleza, con los primeros sistemas expertos. Los primeros estudios sobre *Machine Learning* son de 1959 y florece como estudio independiente en los años 90 del siglo pasado. El *Machine Learning* estaba en los años 60 unido a la inteligencia artificial aunque luego se segrega. Algo semejante ocurre con las redes neuronales. Internet aparece en 1969 para interconectar centros de proceso de datos de la defensa en EEUU; a partir de 1983 inicia un rápido desarrollo en el ámbito civil sumándose muchas universidades de todos los continentes y empresas, sobre todo multinacionales. Esta expansión se vuelve exponencial hasta llegar hoy a todos los rincones del mundo con el diseño de la *World Wide Web* por Tim Berners-Lee en el 1989 y la aparición de los primeros navegadores algunos años más tarde.

Este enorme impulso de las tecnologías de la información y la comunicación en los últimos años, que nos ha abierto posiblemente las puertas a una nueva era —a una nueva etapa de la historia—, ha supuesto no sólo un cambio sino una decisiva contribución al avance en la competitividad de las empresas, en la eficacia de las Administraciones Públicas y en la mejora del funcionamiento de los servicios públicos y del mercado de trabajo. También las TIC han permitido en muchas ocasiones la reducción de brechas sociales y territoriales —en zonas rurales— para facilitar el acceso a la información y a la cultura. Recientemente, la pandemia provocada por el virus SARS-CoV-2 causante de la enfermedad respiratoria COVID-19 ha supuesto un impulso quizás definitivo para el teletrabajo y para la introducción de las tecnologías en la educación y en la sociedad. En ese contexto también han surgido distintas iniciativas tecnológicas para responder a esta emergencia sanitaria que facilitan la comunicación con las personas contagiadas y su localización para garantizar el cumplimiento de las medidas de confinamiento. Estas iniciativas pueden resultar más eficientes que el recurso a los instrumentos manuales —los detectives del conoravirus— para llevar a cabo el rastreo de los contactos o para comunicar posibles contagios, algo que debe ser realizado en el menor tiempo posible de manera que se evite la extensión de la epidemia.

Una de las lecciones aprendidas de esta crisis sanitaria y de los retos a los que se enfrentan todos los países en los próximos años es la necesidad de acometer un fortalecimiento de los sistemas de salud —salud pública y epidemiología, atención sanitaria e investigación biomédica—. Sin embargo, los recursos económicos de los que dispone un Estado social para incrementar la inversión en salud van a ser siempre limitados. La preocupación por la sostenibilidad financiera del Estado social y por la necesidad de gestionar la salud pública y la atención sanitaria con recursos escasos que condicionan la capacidad de actuación obligan a acudir a los tratamientos de datos personales. Por eso es imprescindible, como más adelante señalaremos, que la Unión Europea impulse una estrategia de datos. La Administración Pública no puede prescindir del enorme capital que posee en datos e información para desarrollar sus políticas públicas, en especial de salud. Los tratamientos de datos personales, como hemos señalado en muchas ocasiones, son esenciales para impulsar de una manera eficiente la salud pública, la atención sanitaria y la investigación. A las iniciativas ya ejecutadas relativas a la historia clínica electrónica y a la receta electrónica, hay que sumar en esta nueva etapa el *Big Data*, la inteligencia artificial y el uso de una analítica de datos para identificar necesidades y asignar recursos que estén destinados a mejorar la salud pública, la atención sanitaria de los pacientes y la investigación, al mismo tiempo que favorezcan la eficiencia en el uso de los recursos públicos y privados.

Sin embargo, el desarrollo y la generalización de estas nuevas tecnologías de la información y de las comunicaciones han supuesto un incremento exponencial de los tratamientos de datos personales —Internet de las cosas, nanotecnología, historia clínica electrónica en la nube, RFID— que suponen una amenaza para la

privacidad y para los derechos de las personas. Hay que recordar que los riesgos no se derivan principalmente de los datos personales sino de los tratamientos por lo que el derecho fundamental a la protección de datos personales no tiene como objeto proteger de manera aislada los datos sino únicamente los datos personales sometidos a tratamiento. Además, los riesgos de esta era de Internet provienen no sólo de las Administraciones Públicas sino también de las corporaciones privadas y de los particulares. Dejamos de lado ahora la llamada *Darknet* —red oscura— o *Deep web* —la Internet profunda— donde se aloja la inmensa mayoría del contenido de Internet y que ofrece refugio a los delincuentes internacionales relacionados con las drogas y a las redes internacionales de pedófilos. La mayoría de los afectados no son conscientes de los riesgos que corren sus derechos personales, en especial, la protección de datos personales con las redes sociales, la computación en la nube, la comercialización de datos con tarjetas de cliente, las compras y pagos por Internet, etc. En estos casos se revelan voluntariamente muchos datos personales sobre hábitos y el comportamiento de los consumidores que, sin duda, se negarían a las autoridades estatales —Hufen—. Además, al incremento de las tecnologías en la Administración Pública y en las empresas hay que sumarle sobre todo no sólo su incorporación sino su ocupación —su conquista— de todos los espacios privados de las personas. Como señala el Tribunal Constitucional Federal Alemán en la Sentencia de 27 de febrero de 2008 sobre búsquedas en línea, «los recientes avances en la tecnología de la información han dado lugar a la ubicuidad de los sistemas de tecnología de la información y su uso es fundamental para la forma en que muchos ciudadanos viven sus vidas». Muchos datos personales son objeto de innumerables tratamientos que pasan inadvertidos a los usuarios. De nuevo, esto ha vuelto a ser anticipado por el Tribunal Constitucional Federal Alemán que ha subrayado que estos avances no sólo se han materializado en la capacidad de rendimiento de los ordenadores personales, que pueden ser utilizados para distintos propósitos como administración y archivo de asuntos personales —incluso de negocios—, para biblioteca digital o como dispositivo de entretenimiento, sino también en los numerosos objetos que las personas emplean en su vida cotidiana —*smart phones*, equipos de telecomunicaciones, dispositivos electrónicos en hogares o en vehículos— que contienen componentes de tecnología de la información cuya importancia aumenta si están conectados en red. Esta creciente difusión de los sistemas de tecnología de la información en red, que sin duda ofrece nuevas posibilidades para que el individuo desarrolle su personalidad, también supone nuevos riesgos para la misma. Además de los datos que el usuario de la computadora crea o almacena conscientemente, «en el marco del procesamiento de datos, los sistemas de tecnología de la información también generan automáticamente muchos otros datos que, al igual que los datos almacenados por el usuario, pueden evaluarse en relación con el comportamiento y las características del usuario. Como resultado de ello, en la memoria principal y en los medios de almacenamiento de esos sistemas se puede encontrar una gran cantidad de datos relativos a las circunstancias personales, los contactos sociales y las

actividades del usuario. Si estos datos son recopilados y evaluados por terceros, se pueden extraer conclusiones de gran alcance sobre la personalidad del usuario, hasta la formación de un perfil» —BverfGE 120, 274; Epping—.

Este incremento exponencial de los tratamiento de datos personales se ha hecho especialmente visible en el ámbito laboral —video vigilancia, geolocalización, biometría, etc.—, lo que ha dado lugar a la aparición masiva de nuevos riesgos tanto sobre el derecho fundamental a la protección de datos personales de los trabajadores, considerado como derecho autónomo, como sobre otros derechos fundamentales de los trabajadores de los que la protección de datos personales es en muchas ocasiones una garantía institucional o de instituto. Buena muestra de ello es que muchos de los derechos digitales regulados en el Título X de la LOPDGDD son derechos digitales de los trabajadores como el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo o el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Además, la LOPDGDD recoge en su Título X nuevos derechos digitales de los trabajadores independientes del derecho a la protección de datos personales como el derecho a la desconexión digital en el ámbito laboral o el derecho a la protección de la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador.

El enorme desarrollo de las TIC en los últimos años permite fácilmente suponer que nuestros datos personales son *res in commercio*, objeto de negocio jurídico y, por tanto, que forman parte del patrimonio de una persona —serían *res in patrimonio* en expresión de Gayo—. Admitir la posibilidad de comerciar con nuestros datos personales conlleva también aceptar que sea legítimo intercambiar datos personales por medicamentos, por servicios sanitarios o por un descuento en una póliza de seguro o, incluso para conseguir un trabajo o mantenerlo. Este planteamiento, que sitúa la protección de datos personales en la esfera del derecho de propiedad —los datos personales como una *quasi* propiedad, como diría Esser, siguiendo tanto a los juristas romanos como a los del *Common Law*—, y que se manifiesta en convertir el consentimiento del interesado en el principio jurídico fundamental, genera una enorme brecha, no sólo social sino de derechos, entre los pobres que comercian con sus datos personales y los ricos que no se ven obligados a compartir sus datos personales. Este planteamiento convierte la privacidad en un lujo y condena a los pobres a no tener privacidad. Esta idea trasladada al ámbito del trabajo diferencia entre los trabajadores que se ven resignados a trabajar sin privacidad y los empleadores, agudiza el desequilibrio existente en las relaciones laborales y condena a los trabajadores a no tener privacidad. Sin embargo, los derechos fundamentales, también el derecho a la protección de los datos personales, y, en especial, los derechos de los trabajadores han surgido para proteger a los más débiles en el ámbito de las relaciones jurídicas y laborales. Por tanto, corregir los desequilibrios y proteger a los más débiles —migrantes, trabajadores, menores, personas con discapacidad, personas mayores— debe ser siempre una de las prioridades porque es en última instancia lo que justifica el

derecho y la acción de los poderes públicos. El derecho a la protección de datos personales no tiene en el consentimiento del interesado su principio jurídico fundamental pues es mucho más que un derecho a la autodeterminación informativa y obliga a respetar otros principios y derechos de protección de datos, en especial el principio de calidad y proporcionalidad. Por ello, es necesario continuar el desarrollo normativo del derecho fundamental a la protección de datos personales para poder disponer de un marco jurídico que garantice a las personas —especialmente a las más débiles— el control sobre sus datos personales sometidos a tratamiento.

Son muchas las amenazas que provienen de los avances tecnológicos, especialmente para los menores. Internet les ofrece el acceso inmediato a un mundo que no siempre se ajusta a su nivel de madurez y que puede afectar al libre desarrollo de su personalidad. La introducción masiva de las tecnologías en la educación puede incidir en el aprendizaje de manera que el exceso de información y la tendencia a la reproducción de textos no deje espacio suficiente para la comprensión y para la reflexión crítica. Los jóvenes se acostumbran a emplear la tecnología como entretenimiento y a responder solo a estímulos audiovisuales, lo que anuncia ya la llegada del *homo videns*, del que nos prevenía Sartori. También los mayores poseen cada vez más una cultura de titulares y prefieren los mensajes breves y claros —o los vídeos— y saltan la pantalla de los textos largos más matizados, que obligan a «sumergirse en lo complejo, en lo paradójico, en la política de verdad». En nuestras democracias las nuevas tecnologías han favorecido la transparencia administrativa, el acceso a una información pública veraz en el mundo de la posverdad y la fiscalización del poder; han mejorado la participación en los asuntos públicos, reduciendo las diferencias entre políticos y ciudadanos y multiplicando los espacios individuales de generación de opinión. Sin embargo, como hemos señalado recientemente, la red no es el escenario más apropiado para una democracia deliberativa. La deliberación política requiere la exposición de los propios argumentos y la escucha atenta de los argumentos de los otros, lo que favorece el conocimiento, el respeto y la aceptación del otro; ayuda a crear una cultura del acuerdo y contribuye a acotar los desacuerdos; permite armonizar intereses distintos e incluso contrapuestos y alcanzar objetivos comunes. La deliberación y el continuo ejercicio del diálogo favorecen la inclusión del otro y permiten un consenso cultural de fondo. En cambio, las tecnologías no ofrecen plataformas propicias para la deliberación política y para el diálogo. La limitación de caracteres de algunas herramientas, unida a la superficialidad del hombre contemporáneo, reduce el discurso político en Internet al adoctrinamiento, al argumentario breve, cuando no al mero slogan, que tiene como destinatario la propia parroquia. El *retargeting* digital, a través del cual *Google* te ofrece noticias que te interesan en virtud de unas búsquedas anteriores, favorece la generación de identidades aisladas, que no se comunican entre sí, no reducen distancias, no hacen desaparecer los prejuicios, no aumentan la tolerancia, no permiten la aceptación social del otro. La red se utiliza para procesos plebiscitarios de decisión colectiva,

sin debate, sin argumentación, lo que, en el fondo, encubre movimientos de adhesión o de exclusión, propuestos por los mismos que desdeñan la democracia representativa. Por eso, la red, que es un espacio adecuado para el acceso a la información, para la rendición de cuentas y para el control del poder, no lo es para la deliberación política y para sus frutos que es el acuerdo político, que requiere el diálogo, el respeto y el conocimiento del otro.

Es, por tanto, necesario que el hombre moderno, al mismo tiempo que utiliza las nuevas tecnologías, venza la tendencia al sensismo y al inmediatismo y supere uno de los problemas de la cultura actual que es la ausencia de interioridad y la falta de contemplación —Juan Pablo II—. Al mismo tiempo, se hace necesaria la formación para un uso ético y responsable de las nuevas tecnologías que recuerde al hombre y a la mujer que sus decisiones en Internet deben ser fruto de una responsabilidad moral con los próximos y con la sociedad.

CAMINO VIDAL FUEYO

Es lugar común poner de relieve la extraordinaria y vertiginosa evolución de los avances tecnológicos en las últimas décadas y su correlativa incidencia en distintos ámbitos de la vida privada. Tampoco resulta una novedad constatar que el desarrollo tecnológico crece de manera exponencial, a un ritmo mucho más rápido que el de las normas jurídicas. Por todo ello, mi primera consideración toma forma de pregunta: ¿son suficientes las garantías jurídicas previstas en la teoría general clásica de los derechos fundamentales para defender la privacidad de las personas en un mundo digital sin contornos precisos y sin fronteras geográficas?

Si entendemos que no se puede concebir la ciencia jurídica al margen de los hechos, ni de los fenómenos sociales, ni de los avances tecnológicos, resulta fácil concluir que la tarea del jurista no puede llevarse a cabo exclusivamente desde la unilateralidad formal de la norma, pues sólo a partir de un conocimiento realista y objetivo de los casos en que la tecnología invade y limita nuestros derechos fundamentales es posible articular mecanismos (jurídicos o de otra naturaleza) para hacer frente a las amenazas que de ella emanan. Con esta finalidad, y al objeto de enriquecer mis respuestas a las preguntas número uno y tres de esta encuesta, he contado con la inestimable ayuda de Fernando Fernández-Miranda, experto en nuevas tecnologías y Derecho (socio del Área de Regulación Digital de PwC) que, desde el conocimiento práctico, me ha proporcionado innumerables ejemplos que ponen de relieve la amenaza que los avances tecnológicos pueden suponer para la intimidad y la vida privada de las personas, mostrando un escenario abrumador: la industria 4.0, la robótica y la automatización drástica de procesos, el *big data*, la inteligencia artificial, el internet de las cosas, la realidad virtual, la prestación de servicios de *cloud computing*, los dispositivos de geolocalización y de reconocimiento de datos biométricos, los drones de vigilancia, las *smarts cities*, la tecnología *blockchain*, etc.; insistiendo en que todas estas tecnologías disruptivas

son evidentes manifestaciones de que el actual paradigma tecnológico gira en torno al colosal y sigiloso acceso a nuestros datos personales para correlacionarlos y extraer conclusiones no perceptibles a primera vista para los ciudadanos —desde preferencias personales a tendencias políticas o socio-económicas—, pero que suponen una capacidad de intromisión e influencia en la vida privada de las personas sin precedentes en nuestra historia.

Asimismo, Fernández-Miranda indica que, desde una perspectiva política, el caso de *Cambridg Analytics* es un claro ejemplo de cómo la captación y tratamiento masivo de datos personales y perfiles de ciudadanos de forma ilegítima puede dar como resultado la generación de modelos y algoritmos que permitan unos resultados concluyentes en procesos electorales. En este caso, el acceso ilegal a más de 50 millones de usuarios de Facebook para configurar perfiles psicológicos y lanzar mensajes específicamente diseñados para ciertas audiencias resultó determinante para influir en el voto final y que Donald Trump ganara las elecciones norteamericanas en noviembre de 2016. Lo que resulta significativo, desde el punto de vista de la privacidad, es que este tipo de prácticas tienen como objetivo influir en la opinión a las personas no mediante argumentos, sino a través del «dominio informativo» basado en el previo tratamiento masivo y analítico de sus datos personales, sin su consentimiento.

Desde el punto de vista comercial, la aplicación de algoritmos de aprendizaje automático (*machine learning*) para analizar datos personales a gran escala y en tiempo real (*big data*), como pueden ser hábitos de navegación web, histórico de compras, geolocalización, transacciones bancarias o preferencias en redes sociales (*likes o follows*), permite la elaboración de perfiles de usuarios para abastecer el marketing digital. Sin embargo, la elaboración de estos perfiles conlleva la generación de información complementaria que no ha sido directamente facilitada por los interesados, con el fin de disponer de modelos de conducta o pronósticos sobre su comportamiento o intereses futuros y, lo que es más grave, en ocasiones da lugar a situaciones de discriminación o provoca perjuicios importantes, como consecuencia de la falta de veracidad, exactitud o actualización de los datos utilizados. Pensemos, por ejemplo, en la imposibilidad de acceder a un crédito o a otro tipo de financiación, en la exclusión *a priori* en un proceso de selección laboral o en la denegación de cobertura de una póliza de seguro.

Por último, es necesario hacer una breve referencia al contexto actual de pandemia global en el que nos encontramos como consecuencia de la crisis sanitaria provocada por el coronavirus SARS-CoV-2 (Covid19), pues muchas de las medidas que se están implementando para atajar la propagación del virus afectan al derecho fundamental a la protección de datos, al servirse de tecnologías que invaden ámbitos de privacidad. Pensemos en el uso de aplicaciones para el seguimiento y control de contagios a través de tecnologías de GPS o *Bluetooth*, al uso de drones para controlar el cumplimiento de las obligaciones de confinamiento o para comprobar el aforo en espacios públicos, el control de temperatura en centros de trabajo y comercios, el reconocimiento facial como medio de identificación y autenticación

en relaciones electrónicas y a distancia, la eventual creación de un pasaporte sanitario digital que acredite que el portador no se encuentra contagiado o está presuntamente inmunizado por haber pasado la enfermedad, el uso de aplicaciones de diagnóstico de Covid-19 basados en la sintomatología del usuario, etc.

En consecuencia, las amenazas son muchas y, como se expondrá en las siguientes líneas, la capacidad de las normas jurídicas muy limitada, aunque necesaria.

2. *¿Considera que el reconocimiento de un derecho fundamental es el medio más adecuado para hacerles frente? Desde una perspectiva más general ¿qué reflexiones cabe hacer sobre las posibilidades con las que cuentan el Estado y el Derecho para hacer frente a amenazas de ese tipo?*

LORENZO COTINO HUESO

La garantía de un derecho fundamental en principio resulta la máxima más importante que puede conferir un Estado de Derecho. Así las cosas, desde los años 80 se ha ido construyendo un derecho fundamental de protección de datos. Obviamente ello ha tenido reflejos muy positivos en el ordenamiento español y europeo. Entre otras cuestiones la naturaleza iusfundamental implica unas garantías normativas a través de la acción del legislador, que en España vienen dándose con leyes orgánicas desde 1992. También ha sido bastante positivo que esta especial protección se articule a través de autoridades independientes, que no han hecho más que ganar relevancia con el paso de los años.

Dicho lo anterior, que no es poco y no puede menospreciarse, en general en Europa y en particular en España el tratamiento de la protección de datos alrededor de un derecho subjetivo ha sido bastante negativo. Ello se aprecia con claridad por el hecho de que el consentimiento sea la columna vertebral de este derecho subjetivo. Y la realidad es que otorgar el consentimiento ha devenido en una absoluta rutina masiva. Una sociedad infantilizada y cautivada por la tecnología *ha vendido su alma al diablo* a través de facilitar el consentimiento y de hecho lo que era una garantía ha sido totalmente contraproducente. Algo muy similar ha sucedido con los múltiples derechos (acceso, rectificación, supresión, oposición, etc.). Su ejercicio por la ciudadanía ha sido irrisorio y en modo alguno se ha demostrado una garantía eficaz. La transparencia y suficiente información sobre el tratamiento de datos por el responsable sin duda sigue siendo una garantía muy importante, pues es también un mecanismo preventivo. No obstante, la facilitación de información para efectuar un tratamiento se ha convertido en un ritual rutinario para la ciudadanía. La aceptación de las *cookies* es posiblemente su máxima expresión. Así pues, una visión especialmente subjetiva de la protección de datos ha conllevado una real desprotección de manera aparentemente legítima y legal.

No obstante, el problema aún ha sido mayor. Subrayar un derecho subjetivo fundamental ha llevado a dejar en la sombra sin protección jurídica una visión que trasciende al individuo y sus derechos subjetivos. Las nuevas tecnologías especialmente los grandes datos, el Internet de las cosas y la inteligencia artificial no solo amenazan los derechos de cada una de las personas cuyos datos se tratan. Los nuevos tratamientos masivos con perfilados y algoritmos crean de manera continua colectivos de miles, cientos de miles o millones de personas que comparten diversas cualidades y que son objeto dinámicamente de un trato y decisiones diferentes. Asimismo, muchos de los tratamientos se realizan sobre datos anonimizados o seudonimizados, que no permiten la identificación de las personas concretas titulares de derechos. En consecuencia, formalmente, no queda afectado ni el derecho de protección de datos ni posiblemente otros derechos individualmente, a nivel *micro*, por decirlo de algún modo; pero materialmente las decisiones públicas y privadas que se adoptan sí que impactan —a nivel *macro*— en la sociedad en general, en grandes colectivos y en su protección de datos y otros derechos fundamentales y en bienes constitucionales esenciales para el Estado social y democrático de Derecho. Sin embargo, estos impactos no están siendo guarnecidos por un derecho bajo la reduccionista perspectiva de derecho subjetivo que captura toda la atención.

Como respuesta dogmática, tanto la preservación de la dignidad de la persona, cuanto la dimensión objetiva de los derechos fundamentales, generan unos deberes de protección que irían más allá del titular sujeto del derecho. Asimismo, no son nuevos diversos mecanismos jurídicos como las acciones de protección de colectivos e intereses difusos. Sin embargo, esta protección no se deriva propiamente del contenido el derecho subjetivo. Es necesaria una acción legislativa que hasta ahora ha quedado muy a la sombra del derecho subjetivo de protección de datos.

Precisamente, los mayores avances en los últimos tiempos se deben a una nueva visión preventiva de la protección de datos bajo la responsabilidad proactiva, la privacidad en el diseño y por defecto, la responsabilidad demostrada, las evaluaciones de impacto o la figura de los delegados de protección de datos. Todo ello ha sido incluido o reforzado por el Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD). Y precisamente este tipo de garantías, al menos hoy por hoy, no aparecen claramente conectadas con el derecho subjetivo de protección de datos.

Por último, hay que añadir que se ha construido un *nuevo* derecho de protección de datos, distanciándolo de la privacidad y la intimidad. Sin embargo, en ocasiones resulta absurdo, inviable o contraproducente desvincular la protección de datos de la privacidad que es su matriz y en la que sin duda se integra. De hecho, una visión más amplia a partir de la privacidad es la mejor estrategia para hacer frente de manera dinámica a los nuevos retos. Es más, la UE está yendo más allá y recientemente aborda la cuestión con un enfoque más general de la responsabilidad por daños (Libro blanco y Estrategia de la Comisión Europea de febrero de 2020).

ROSARIO GARCÍA MAHAMUT

Adecuado, sin duda; exclusivo, en absoluto. Uno de los problemas a la vez que retos más acuciantes para hacer frente a las amenazas que se ciernen sobre los distintos derechos de las personas es precisamente la obligación de reconocer lo que aporta «el avance tecnológico» al servicio de la sociedad y de las personas en todos los ámbitos, con la misma conciencia y reconocimiento de que el uso, finalidad y diseño puedan no ya conculcar derechos fundamentales subjetivos de las personas, sino algo mucho más grave: socavar y conculcar los principios y valores fundamentales sobre los que se erige y que perfectamente identificamos como Estado Social y Democrático de Derecho. Conocimiento y reconocimiento de las amenazas es la herramienta más potente con la que contamos. Educación tecnológica y una tecnología conocedora de los derechos y de los límites deberían ser el binomio básico de una cultura de la protección de los datos. Una vez más, educación sobre lo que significa la protección de nuestros datos y reconocimiento e identificación de los límites de un derecho que tampoco es absoluto sigue siendo la herramienta crucial para aprovechar todas las oportunidades que ofrece la evolución tecnológica a la vez que para afrontar los riesgos que comportan para una sociedad digitalizada.

Responder a la segunda cuestión exige ser absolutamente conscientes de que el Derecho siempre regulará de forma obsolescente una evolución tecnológica que minuto a minuto deviene obsoleta también. El analfabetismo tecnológico no puede acompañar a ninguna suerte de normativa garantista superior. Las amenazas no se ciernen exclusivamente contra derechos concretos de personas concretas; impactan directamente en los principios y valores sobre los que descansa la propia existencia del Estado Democrático de Derecho. Pienso, por ejemplo, en el uso del *big data*, la inteligencia artificial, la aplicación del *microtargeting* en los procesos electorales que pueden llevar a la manipulación de las personas mediante la realización de perfilados exhaustivos, amén, obviamente de las «fake-news» y la «desinformación online», citando ejemplos elementales.

Por todo ello, creo firmemente que se ha finiquitado una época y el método jurídico exige ser reformulado en sus diversos compartimentos estancos. La interdisciplinariedad, la multidisciplinariedad y la transdisciplinariedad constituye una exigencia metodológica ineludible que debemos afrontar para, desde la seguridad jurídica, poder garantizar de la forma más eficiente un opulento y eficaz sistema de garantías.

Pero no solo eso, conviene insistir en una formación continuada de la ciudadanía, de los poderes y autoridades públicas, del sector privado y, cómo no, de todos los operadores jurídicos y aplicadores del derecho, de los riesgos reales que se corren y de los límites y garantías de los derechos que nos asisten. El ciberespacio no puede quedarse al margen de una formación técnica y jurídica básica.

PABLO LUCAS MURILLO DE LA CUEVA

Los derechos fundamentales son la respuesta jurídica a las demandas de satisfacción de las necesidades esenciales que plantea la vida en sociedad. Aseguran las que en otro tiempo se llamaron condiciones indeclinables para la convivencia. Detrás del reconocimiento de cada derecho fundamental hay una historia de negación y de reivindicación de los medios para satisfacer esas necesidades. Ya sea la libertad personal, la de conciencia o la de huelga, por poner algunos ejemplos. La necesidad esencial a la que responde este derecho es la autodeterminación informativa, el control por cada persona del acceso, tratamiento y uso por terceros de la información que le concierne.

El Derecho, como en todos los casos en que la conducta de unos puede perjudicar a otros, busca ofrecer el punto de equilibrio para que el ejercicio de una actividad lícita y necesaria, en este caso, la de hacerse con, tratar y comunicar información personal, no se traduzca en consecuencias perjudiciales para las personas a las que corresponde esa información. Así dicho, parece tarea sencilla pero no lo es en absoluto. La mejor prueba la encontramos en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales. El primero, del que la segunda viene a ser un complemento, es un texto jurídico de gran complejidad porque enormemente complejo es llegar a ese equilibrio.

Además, las posibilidades de alcanzarlo vienen condicionadas de origen. De un lado por el vertiginoso desarrollo de las tecnologías de la información y de las comunicaciones que hacen realidad de un día para otro lo que antes parecía imposible. El Derecho va más que nunca a remolque de ese progreso. De otro lado, contribuye a dificultarlo el contexto en que se produce el reconocimiento del derecho a la protección de datos. Aquí vuelvo al Reglamento (UE) 2016/679. Parece contemplarlo como un límite a la libertad de circulación de información personal. Cierto que no hay derechos ilimitados, ni siquiera los derechos fundamentales lo son y también es cierto que los derechos se limitan recíprocamente entre sí, pero es igualmente verdad que no es lo mismo proclamar un derecho en cuanto tal —al fin y al cabo es lo que hace la Carta de los Derechos Fundamentales— que presentarlo como un límite de otro.

La opción del Reglamento (UE) 2016/679 se explica porque busca conciliar la protección de los datos personales con los intereses de quienes se dedican a tratarlos y transmitirlos para los más variados fines. Pretende fortalecer la posición de los afectados y, al mismo tiempo, establecer un marco jurídico homogéneo en la Unión Europea y, además, claro para la circulación de la información personal. El resultado conseguido es estimable porque ha dotado al derecho fundamental reconocido por la Carta de una consistencia que no tenía antes bajo la Directiva 95/46/CE, ni siquiera con la interpretación que de ella hizo el Tribunal de Justicia en sus sentencias de 2014 y 2015 en los asuntos Digital Rights Ireland,

Google contra España o Schrems. No obstante, tiene el condicionante desde el punto de vista de los principios de que parece concebirlo como un derecho subordinado a la libertad de circulación de los datos. El alcance que en la práctica adquiera esa relación, es decir el peso relativo que gane en ella cada uno de los dos elementos concernidos es algo que habrá que comprobar en el futuro.

A la dificultad técnica que resulta de la especialidad del objeto y de la complejidad de la regulación, se une el obstáculo que suponen las fronteras estatales. Superada en la Unión Europea, gracias al régimen común del Reglamento (UE) 2016/679, la disparidad legislativa que, pese a la Directiva 95/46/CE, pervivía en su interior, fuera de ella nos encontramos con Estados en los que el derecho a la protección de datos no está reconocido o no cuenta con una garantía equivalente a la que asegura la Unión Europea. Estas circunstancias son aprovechadas para eludir las exigencias que imponen ahora el Reglamento (UE) 2016/679 y las leyes nacionales que lo complementan pues las fronteras marcan el límite espacial a la vigencia de las normas pero no detienen los flujos de información que circulan por las redes. Por eso, mientras no se disponga de una regulación universal susceptible de ser aplicada en todo el mundo no será posible establecer la plena protección de este derecho fundamental.

Por último, pese al tiempo transcurrido desde que entraron en vigor las primeras leyes de protección de datos personales, sigue sin existir el suficiente conocimiento de los peligros que entrañan el acceso a ellos, su tratamiento y uso ilimitados. Falta mucha educación a todos los niveles y todavía no se ha conseguido superar el generalizado desconocimiento por los afectados del perjuicio que se les causa de ese modo que les impide actuar para defenderse. Si el titular del derecho no lo hace valer es muy difícil que su respeto sea una realidad.

MANUEL MEDINA GUERRERO

La complejidad técnica que encierra hacer frente eficazmente a tales amenazas tecnológicas implica que una adecuada tutela de los datos personales escape en buena medida a las categorías clásicas empleadas en la teoría general de los derechos fundamentales.

De hecho, un elemento central de su sistema de garantía es la existencia de un organismo independiente especializado al que se encomienda en primera instancia la tarea de supervisar la observancia de la normativa. La presencia de esta institución constituye —por decirlo así— un integrante del «contenido esencial» del derecho en la esfera de la Unión Europea (en este sentido, el Considerando 117 del RGPD, que sigue de cerca lo ya declarado en el Considerando 62 de la Directiva 95/46/EC). De ahí que la consagración de este derecho como derecho autónomo en la Carta de Derechos Fundamentales de la Unión Europea se erija sobre la premisa de que el respeto de su normativa reguladora «*quedará sujeto al control de una autoridad independiente*».

Que el sistema de tutela de los datos personales no se circunscribe a los contornos tradicionales de un derecho fundamental, es una apreciación que se hace evidente con la sola lectura superficial del RGPD. Es todo un denso entramado de obligaciones de organización y procedimiento el que configura el perfil último de su régimen tuitivo. En efecto, el nuevo sistema implantado en el RGPD se asienta y articula sobre el principio de responsabilidad proactiva, que presupone un nuevo enfoque o aproximación en la protección de los datos personales. El anterior modelo ponía el acento en el establecimiento de reglas y estándares mínimos en la gestión de la información, y contemplaba vías de reparación a posteriori, esto es, cuando ya se había producido la vulneración de la privacidad. Por el contrario, bajo el enfoque «proactivo» ahora vigente, se trata precaver y evitar por anticipado que aparezcan quiebras de privacidad y el correspondiente daño para los afectados, en lugar de ofrecer únicamente mecanismos para la reparación de los perjuicios causados. Se trata, en suma, de que sean las propias entidades obligadas las que adopten las medidas para minimizar los riesgos de vulneración de la privacidad y estén en condiciones de demostrar que han operado diligentemente al respecto. Y a la consecución de dicho objetivo de la «proactividad» sirven directa o indirectamente la mayor parte de las exigencias, medidas y previsiones que jalonan el nuevo marco normativo: nombramiento de un delegado de protección de datos, registro de actividades de tratamiento, análisis de riesgos, evaluaciones de impacto, impulso de códigos de conducta, mecanismos de certificación, etc. Así, pues, la adaptación al nuevo modelo impone a los sujetos obligados la asunción de nuevas cargas y tareas, así como ajustes en su propia organización.

ARTEMI RALLO LOMBARTE

Durante casi tres décadas, el derecho a la protección de datos ha ostentado en exclusiva el honor de desarrollar el mandato del art. 18.4 CE y las garantías de los derechos frente a los avances tecnológicos se han vertebrado en torno a un derecho a la protección de datos al que se le dotó, desde sus orígenes, de una potencia normativa extraordinaria que culminó con su consagración como derecho fundamental autónomo en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea. En el plano nacional, la aprobación de la Directiva 95/46/CE dio paso a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y, simultáneamente, el Tribunal Constitucional consagró un derecho fundamental autónomo a la protección de datos personales y le otorgó un inequívoco contenido esencial (SSTC 290/2000 y 292/2000). Este reconocimiento por la jurisprudencia constitucional de un derecho fundamental autónomo a la protección de datos personales sirvió de auténtica punta de lanza del mandato constitucional dirigido a los poderes públicos para limitar el uso de la tecnología en garantía de los derechos.

La fuerza expansiva del derecho fundamental de protección de datos ha permitido durante muchas décadas canalizar y limitar los posibles riesgos provocados por la tecnología pero su enorme potencialidad ya no alcanza a todos los ámbitos en los que hoy se proyectan estas amenazas. Como hemos argumentado en un trabajo bien reciente («Una nueva generación de derechos digitales», *Revista de Estudios Políticos*, 2020, 187, pp. 101-135), este manto protector parece no dar más de sí para cubrir y amparar otras muchas amenazas y riesgos que operan, al margen de la información personal, en la realidad digital sobre derechos y libertades individuales.

Por ello, el art. 18.4 CE adquiere de nuevo pleno sentido más allá de la acotada preocupación por garantizar la protección de datos y reclama una decidida acción legislativa dirigida a reconocer y garantizar los derechos digitales, esto es, los derechos y libertades individuales afectados por la realidad digital. La referencia a *la informática* en el texto constitucional de 1978 resultó altamente meritoria por vanguardista y por otorgar trascendencia constitucional a la necesidad de proteger al individuo frente a los primeros avances tecnológicos. Durante décadas, la esfera aplicativa de este precepto ha quedado circunscrita al ámbito de la protección de datos personales. Las distintas leyes de protección de datos siempe han sido calificadas como las normas de desarrollo de este precepto constitucional, con una apariencia de exclusividad excluyente, como si en el ámbito de protección de este precepto únicamente cupiese la garantía del derecho de protección de datos. Pero esto no es así. Este precepto tiene un impacto general habilitador de una completa legislación dirigida a garantizar derechos digitales entre los que el de protección de datos ocuparía una posición central. Sin embargo, el mandato del art. 18.4 CE adolece de las limitaciones inherentes a su propia naturaleza: una genérica habilitación al legislador para reconocer y regular derechos digitales sufrirá las debilidades propias de este rango normativo y someterá a discreción legislativa su tipología y contenidos básicos.

Cuatro décadas después de producirse la visionaria decisión del constituyente, la hipotética reforma del texto constitucional sería la mejor respuesta para constitucionalizar estos derechos digitales otorgándoles las garantías necesarias para hacer frente a los riesgos que acompañan la revolución tecnológica atendiendo la demanda social de protección de la dignidad humana frente a los riesgos y amenazas presentes y futuras que provengan de una tecnología en permanente evolución. Así lo advierte el Preámbulo de la LOPDGDD: «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».

Sin embargo, en tanto no se acometa esa tarea, el legislador tiene la ineludible tarea de reconocer y garantizar *nuevos derechos digitales* (como hace el Título X de la LOPDGDD) para cumplir con el mandato constitucional vigente y dar respuesta a las trascendentes transformaciones tecnológicas que envuelven una sociedad actual en constante desarrollo. La sociedad digital demanda un haz de derechos

que garanticen la subordinación de la tecnología al individuo, preserven su dignidad y se proyecten sobre la totalidad de los ámbitos en que se actúa en sociedad. Los derechos digitales adquieren una dimensión multifacética que residencia tanto en el individuo como en los poderes públicos su garantía efectiva. Garantizar derechos digitales no implica únicamente procurar que los ciudadanos no vean coartada o limitada su capacidad de uso de la tecnología o preservar que los individuos puedan reaccionar haciendo valer sus derechos frente a la tecnología. La garantía efectiva de los derechos en la era digital necesariamente impone obligaciones a los poderes públicos para posibilitar un acceso pleno a las herramientas tecnológicas que permita el desarrollo de su personalidad en el mundo contemporáneo en tanto realidad digital y, en concreto, su acceso al espacio virtual construido sobre la existencia de Internet.

LUCRECIO REBOLLO DELGADO

A mi juicio entran en liza tres elementos esenciales en esta cuestión. El Derecho, el Estado y los derechos y libertades fundamentales. Con carácter individual ninguno tiene entidad suficiente para ser la solución absoluta. El eficaz empleo de los tres elementos debe ser la solución a la nueva problemática que plantea la sociedad digital.

Recordemos que el Derecho parte con unas considerables desventajas intrínsecas con respecto a la evolución de la tecnología. Es eminentemente estatal, y hemos manifestado que las innovaciones tecnológicas han roto la barrera del espacio y el tiempo. Otra característica del Derecho es que surge para solventar un conflicto ya existente, su capacidad predictiva es escasa y con un alto contenido de errores o portillos jurídicos, y en todo caso, normalmente se genera a *posteriori*, una vez constatada la necesidad. Por último, su elaboración está mediatizada por infinidad de actores y de intereses, a lo que se suma su dificultad en la aplicación. En definitiva, el Derecho tal y como lo conocemos en la actualidad, deberá cambiar de forma sustantiva para ser eficaz en esta tarea de solventar problemas en la sociedad digital.

No faltan corrientes que apuntan como solución a este problema la sustitución de códigos normativos por códigos informáticos, lo que supone sustituir las necesidades sociales, o las humanas, por las digitales, circunstancia que, aunque nos parezca de ciencia ficción, está a la vuelta de la esquina, y que a su vez plantea un nuevo conjunto de problemas.

Tampoco el Estado se vislumbra como única posible solución a las problemáticas que plantea la sociedad digital, pero de modo parecido al Derecho, es actor necesario, es parte de la solución. Sus medios tradicionales de actuación —generar normas, ordenar procesos y la capacidad ejecutiva, y en su caso, coactiva, con límite territorial—, no son suficientes en los nuevos desafíos. Sus potestades clásicas no alcanzan para poder controlar o limitar los desequilibrios

o problemas que genera la sociedad digital, dado que esta tiene un carácter universal.

El reconocimiento de los derechos y su garantía eficaz es el elemento troncal en la forma de vida occidental, pero requiere de los otros dos analizados, es necesario insertarlo en una estructura social consolidada como es la de los países democráticos actuales, pero con carácter internacional o globalizado, de lo contrario decaen en su eficacia los tres pilares que hemos referido. Indudablemente, el reconocimiento y garantía de los derechos fundamentales es la única senda de garantía para armonizar el desarrollo tecnológico y los derechos y libertades del ciudadano, y de forma más concreta para la protección de los datos de carácter personal.

ANTONIO TRONCOSO REIGADA

Frente a la primera amenaza que constituía la informática, la Constitución portuguesa de 1976 y la Constitución Española de 1978 así como otras reformas y textos constitucionales de esa época —Finlandia (1980), Países Bajos (1983), Suecia (1994)— plantearon la necesidad de limitar la informática para proteger el derecho a la intimidad y el pleno ejercicio de los derechos. Especialmente interesante fue la primera redacción del art. 35 de la Constitución Portuguesa y sus sucesivas reformas que tempranamente establecieron un derecho del ciudadano a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos y a poder exigir su rectificación y actualización, prohibiendo la interconexión de ficheros y la utilización de la informática para el tratamiento de datos de ideología, religión o relativos a la vida privada. Otros países como Italia y Alemania con Constituciones aprobadas después de la II Guerra Mundial configuraron un derecho a la protección de datos personales a partir de la interpretación constitucional de otros preceptos por sus Tribunales Constitucionales.

Hay que destacar especialmente la ya citada Sentencia del Tribunal Constitucional Federal Alemán, de 15 de diciembre de 1983, que proclamó la existencia de un derecho a la autodeterminación informativa como el derecho de la persona a decidir por sí misma sobre el uso y la divulgación de sus datos personales, dando un nuevo fundamento a la ya existente Ley Federal de Protección de datos. Aunque el derecho a la autodeterminación informativa no está regulado explícitamente en la Constitución Alemana —GG—, el Tribunal Constitucional Federal Alemán lo dedujo a partir del derecho al libre desarrollo de la personalidad —art. 2.1 GG— en relación con el artículo 1.1 GG que recoge la protección de la dignidad humana y la obligación de todo poder público de respetarla y protegerla. La Sentencia señala que «en el centro del orden constitucional se encuentran el valor y la dignidad de la persona, que en la libre determinación actúa como miembro de una sociedad libre. Además de las garantías especiales de

libertad, el derecho general de la personalidad garantizado en el artículo 2.1 en relación con el artículo 1.1 de la Ley Fundamental sirve para proteger estos valores y la dignidad». También subraya que «este derecho puede adquirir cada vez más importancia, en particular en vista de los avances modernos y las nuevas amenazas a la personalidad humana que se asocian a ellos». De esta forma, el Tribunal Constitucional Federal Alemán derivó el derecho a la «autodeterminación informativa» del derecho general de la personalidad —es una forma especial del derecho al libre desarrollo de la personalidad—, asignándole un estatus —un rango— de derecho fundamental. El derecho fundamental del artículo 2.1 GG ha demostrado esencialmente su valor en su función de *catch-all* y como reserva de libertad —Kloepfer. En las condiciones modernas de procesamiento de datos, el libre desarrollo de la personalidad requiere la protección de la persona contra la recopilación, el almacenamiento, uso y divulgación ilimitada de sus datos personales. El vínculo dogmático con el derecho general de la personalidad y la conveniencia de una mayor protección de los datos no debe ocultar el hecho de que el Tribunal Constitucional haya creado un nuevo derecho fundamental y, a este respecto, haya tomado una decisión de gran importancia. Sin embargo, habría sido función del poder de reforma de la Constitución cerrar la laguna en la protección de los derechos fundamentales identificada por el Tribunal Constitucional, dentro un proceso de toma de decisiones en el Parlamento y con un debate público que lo acompañe. En esta dirección, junto con el derecho fundamental a la protección de datos debería incluirse expresamente en la Constitución el derecho al acceso a la información pública como garantía de la libre circulación de la información. Como el derecho fundamental a la protección de datos es el resultado de un desarrollo del Tribunal Constitucional y carece de una base textual, en sentido estricto, deben tomarse de la decisión del Tribunal Constitucional los titulares del derecho, el contenido del derecho y las restricciones del derecho —Ipsen—.

Es interesante analizar también la dirección de la protección. La propia expresión —autodeterminación informativa que elige el Tribunal— pone de manifiesto que se trata de un derecho de estatus negativo, que trata de evitar fundamentalmente la recopilación estatal de datos personales. El derecho fundamental a la protección de datos personales como derecho de libertad se opone, por una parte, a los tratamientos que llevan a cabo los poderes públicos —como se evidencia en la Sentencia sobre la Ley del Censo—. Además, como derecho fundamental no tiene sólo un carácter defensivo sino también una dimensión objetiva e institucional en virtud de la cual el Estado tiene la obligación de impedir, a través de medidas legislativas, que el individuo sea objeto de una recopilación de datos personales. El legislador tiene un deber de protección que se aplica a las transacciones jurídicas privadas por lo que es un derecho fundamental que tiene una eficacia indirecta frente a terceros y supone una limitación a la libertad de contratación por intervención del legislador, especialmente pertinente en el caso de las relaciones contractuales en las que una de las partes contratantes tiene tal

peso «que puede determinar de facto unilateralmente el contenido del contrato» —Sodan—. Por tanto, las leyes de protección de datos cumplen el mandato constitucional de proteger los datos personales que son sometidos a tratamiento tanto por autoridades y organismos públicos como también por personas físicas o jurídicas de Derecho privado. Es relevante la cuestión de la eficacia horizontal del derecho fundamental a la protección de datos personales, especialmente por la situación de fuerte asimetría en este campo. Los agentes económicamente poderosos pueden invocar a menudo los derechos fundamentales con respecto a sus actividades mientras que los agentes económicamente más débiles —los portadores de los bienes protegidos perjudicados por los actores económicamente fuertes— están en muchas ocasiones sólo resguardados por la dimensión institucional del deber del Estado de proteger los derechos fundamentales. Se ha llamado así la atención sobre la economización de los derechos fundamentales, que ha adquirido una importancia desproporcionada porque las grandes empresas y las asociaciones empresariales pueden representar con éxito sus casos ante los Tribunales Europeos y Constitucionales y se están convirtiendo en actores decisivos en la lucha por los derechos fundamentales y sus límites. Así, pues, muchos de los procedimientos ante el Tribunal Constitucional se refieren típicamente a la defensa de los intereses colectivos por medio de los derechos fundamentales, lo que ha traído como consecuencia su desindividualización. «El hombre contra el Estado» parece ser hoy una definición nostálgica de la función de los derechos fundamentales, que está siendo suplantada cada vez más por la «organización contra el Estado» —Kloepfer—. En todo caso, hay que subrayar que, si este derecho a la protección de datos personales tiene su fundamento en la dignidad humana y en el libre desarrollo de la personalidad, tiene también un efecto directo sobre terceros y supone una norma de conducta para todos —Hömig—.

El Tribunal Constitucional Federal Alemán señaló que el individuo no tiene un derecho en el sentido de un dominio absoluto e irrestricto sobre «sus» datos; es más bien una personalidad que se desarrolla en el seno de la comunidad social y que depende de la comunicación. Por ello, el individuo debe aceptar las restricciones a su derecho a la protección de datos personales en virtud de un interés público superior. Estas restricciones requieren de una base constitucional; deben estar previstos en una Ley de forma que sean claras y reconocibles para el ciudadano y que, por tanto, respondan al requisito constitucional de claridad de las normas; y su aplicación debe ser proporcional. Así, «la razón, el propósito y los límites de la injerencia deben definirse de manera específica —para la materia—, precisa y clara» —BVerfGE 113, 348; 128, 1—; como mínimo, debe establecerse «qué organismo estatal está autorizado a reunir o procesar la información en cuestión para cumplir qué tarea» —BVerfGE 118, 168—, también en el ámbito de un expediente de lucha contra el terrorismo —BVerfGE 133, 277—. Esta exigencia de reserva de ley también se aplica a la utilización ulterior de los datos; el nuevo propósito debe estar «regulado con suficiente claridad» —BVerfGE 130, 1—. A este respecto, es necesaria una autorización legal —BVerfGE 65, 1—. Por

último, las intervenciones sólo deben aceptarse si son proporcionadas —BVerfGE 84, 239—, si «se persigue un propósito legítimo con medios apropiados, necesarios y razonables» —BVerfGE 115, 320—. En especial, las restricciones legales al derecho fundamental a la autodeterminación informativa deben corresponder a la prohibición del exceso.

En estos días que se celebra el trigésimo aniversario de la reunificación alemana, es muy interesante comparar los dos regímenes políticos. En la República Federal Alemana y en el marco de la Ley Fundamental de Bonn, el Tribunal Constitucional Federal Alemán estaba en la vanguardia de los derechos, alumbrando el derecho a la autodeterminación informativa en la Sentencia de 1983 que declaraba inconstitucional la Ley del Censo que simplemente solicitaba datos personales para compararlos con los que figuraban en los registros y corregir los errores. Al mismo tiempo, a pocos kilómetros, en la llamada República Democrática Alemana, estaban los archivos de la *Stasi* —hay una viva polémica en Alemania sobre el acceso a esta ingente información sobre personas —BVerwGE 121, 115—, almacenados por un Estado, que se autodenominaba democrático y que mantenía un concepto de «derechos básicos socialistas» que no condujo a ningún derecho efectivo de defensa contra el Estado. «Las violaciones de la dignidad humana (por ejemplo, a través del espionaje de la Stasi o del régimen fronterizo) eran estructurales» —Kloepfer—. Lo que diferenciaba a la República Federal Alemana de la otra República no era la existencia de un Estado, el empleo de la palabra democracia o la apelación genérica a los derechos sino la protección de la dignidad humana y la obligación de todo poder público de respetarla y protegerla —en los ancianos, en los migrantes, en los débiles—, el reconocimiento del derecho a la vida, el libre desarrollo de la personalidad —lo que es contrario a que toda la sociedad esté subvencionada y viva de las prestaciones estatales— y el respeto a la libertad ideológica de manera que ninguna ideología tenga un carácter estatal y sea objeto de una enseñanza obligatoria —Jarass; BVerfG-K, NVwZ 90, 55—, previniendo contra la educación unilateral en la escuela —Starck, Mangoldt—. Este era el centro de la Constitución alemana y, a mi juicio también de nuestra Constitución. Hay que recordarlo porque desaparecen los Estados pero perviven las ideologías.

Siguiendo esta estela alemana, el Tribunal Constitucional de España afirmó de manera progresiva en distintas Sentencias, en especial, en la Sentencia 292/2000, de 30 de noviembre, la existencia en el art. 18.4 CE de un derecho fundamental a la protección de datos personales. Si bien el tratamiento automatizado es el principal objetivo, su ámbito también se extiende al tratamiento no automatizado, aunque esto no se encuentra recogido en el art. 18.4 CE —si evidentemente en el derecho al libre desarrollo de la personalidad —art. 10.1 CE y art. 2.1 GG—. Posteriormente, la Carta de Derechos Fundamentales de la Unión Europea ya proclamó textualmente en el art. 8 que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan», señalando expresamente como contenido los principios de lealtad del tratamiento, de

limitación de la finalidad —«estos datos se tratarán de modo leal, para fines concretos»— y de licitud del tratamiento —«sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley»— y los derechos de acceso y de rectificación —«toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación». Llama la atención la previsión constitucional de la garantía de que «el respeto de estas normas estará sujeto al control de una autoridad independiente», que después abordaremos. Igualmente el Tratado de Funcionamiento de la Unión Europea señala expresamente en su art. 16 que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan», correspondiéndole por tanto al Parlamento Europeo y al Consejo, establecer con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal en el ámbito de la Unión Europea. En virtud de esta habilitación normativa, le ha correspondido al RGPD adaptar el derecho derivado institucional de la Unión Europea sobre el derecho fundamental a la protección de datos personales a los enormes avances producidos en las tecnologías de la información y la comunicación desde la aprobación de la Directiva 95/46/CE, que no fue capaz de regular ni tampoco de entrever esta nueva realidad de Internet, antes mencionada. El RGPD regula el derecho a la protección de los datos de carácter personal, fortaleciendo el control de las personas sobre sus datos personales sometidos a tratamiento y garantizando un nivel equivalente de protección de los datos personales en la Unión Europea. Esto lo hace desarrollando los principios y los derechos de protección de datos y las obligaciones del responsable y del encargado del tratamiento en una norma obligatoria en todos sus elementos y directamente aplicable y mejorando su implementación a través de las autoridades de control.

Sin perjuicio de que el reconocimiento de un derecho fundamental en una Constitución normativa sea el medio más adecuado para proteger a la persona frente a estas amenazas al vincular a todos los poderes públicos —también al poder legislativo—, las posibilidades con las que cuenta el Estado —después analizaremos la dimensión supranacional— y el Derecho siempre son limitadas. Parece que la pregunta nos interpela sobre si existe otro modelo de respuesta. Lógicamente, la otra posibilidad es hacer frente a estas amenazas apoyándonos principalmente en la propia sociedad y en la industria. El modelo norteamericano ha hecho hasta ahora descansar la protección de datos en el ámbito del derecho del consumo, del derecho de la competencia y de la autorregulación de las empresas —las empresas tienen que cumplir con sus clientes sus compromisos de privacidad y si no lo hacen se les puede exigir judicialmente su responsabilidad—. Estas dos posibilidades, lejos de ser alternativas, son complementarias. De hecho, el legislador europeo apuesta también por los elementos de autorregulación como los códigos de conducta, los mecanismos de certificación, el delegado de protección de datos, la privacidad en el diseño —que la privacidad esté presente en el momento del diseño del sistema de información, por ejemplo, en la elaboración

de las especificaciones técnicas y en el desarrollo de los programas o sistemas operativos—, la privacidad por defecto —que las configuraciones por defecto respeten la privacidad—, las tecnologías de protección de la privacidad —PET—, avanzando en este camino más allá de lo que hacía la Directiva 95/46/CE. En gran medida, el RGPD se apoya para el cumplimiento de la normativa de protección de datos en el principio de responsabilidad proactiva y en la *accountability* del responsable del tratamiento. Así, es imprescindible que las instituciones públicas eviten las posiciones frentistas en relación con las empresas y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria —que no deja de ser un *stakeholder*— sino de alcanzar un diálogo que permita una mayor protección de los datos personales. Es necesario introducir la protección de datos dentro de la responsabilidad empresarial, convirtiendo a las empresas —también al buen funcionamiento de sus propios canales de denuncia— en un elemento estratégico en el sistema de garantías, convenciéndolas de que Internet y la protección de datos es un canal de retorno, que la privacidad es algo demandado por los clientes y cuyas quiebras afectan gravemente a la reputación corporativa —como han comprobado tanto empresas proveedoras de servicios de redes sociales como las propias Administraciones Públicas—.

Así el Reglamento se aleja de un modelo jurídico de Derecho continental europeo, que proviene del Derecho romano y que se caracteriza por una amplia regulación y una predeterminación de la solución jurídica, para acercarse también a un modelo de *Common Law*, caracterizado por una mayor desregulación y que tiene en cuenta la valoración del caso concreto por parte del responsable. De esta manera, el RGPD no autoriza a la Comisión ni deja apenas margen de maniobra a los Estados para establecer medidas de seguridad de los tratamientos lo que contrasta con el espacio que sí ofrece a la autorregulación en este ámbito al establecer que la adhesión a un código de conducta o a un mecanismo de certificación «podrá servir de elemento para demostrar» que se adoptan las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado. El RGPD deja la determinación de las medidas de seguridad en manos del responsable a partir de la evaluación de riesgos, animándole a recurrir a esquemas privados de seguridad. En cambio, la LOPD, a diferencia de la legislación de otros países, no se limitaba a señalar que el cumplimiento del principio de seguridad de los tratamientos era una obligación genérica del responsable y del encargado, sino que lo vinculaba a la adopción de unas medidas técnicas y organizativas concretas aprobadas en la normativa. Desde un planteamiento exigente con la calidad de la ley, la seguridad de los datos no podía ser algo indeterminado sino que debía presentar la certeza suficiente que evitase la incertidumbre sobre su modo de aplicación efectiva, algo sobre lo que incidió el voto particular de Pérez Tremps en la STC 17/2013, de 31 de enero —F. J. 3.º— que cuestionaba que «aunque la norma prevé que el acceso se realizará con las máximas medidas de seguridad, éstas no se concretan».

Evidentemente, la introducción de elementos de la cultura jurídica anglosajona, como la autorregulación, la desregulación y la *accountability*, si bien aporta

una mayor flexibilidad a la hora de buscar soluciones al caso concreto y de adaptarse a los futuros cambios tecnológicos, también supone una mayor inseguridad jurídica para aquellos responsables acostumbrados a la detallada y extensa regulación característica del modelo jurídico continental. Algo semejante ocurre en el ámbito de la supervisión, función que el RGPD no atribuye en exclusiva a la autoridad de control, sino que también se desarrolla dentro de los códigos de conducta y de los esquemas privados de certificación. Sin embargo, la autorregulación representa únicamente una solución complementaria y no puede ser la garantía principal sobre la que descanse la privacidad de los usuarios. Las empresas se siguen moviendo frecuentemente por lógicas económicas a corto plazo. Las normas jurídicas han surgido, de hecho, como garantía de la privacidad frente a las malas prácticas de las empresas. Por ello, un riesgo siempre presente es que una apuesta excesiva por los elementos de autorregulación y un desfallecimiento en la actividad de control afecten en este ámbito a las funciones públicas de soberanía y supongan una *privatización de la regulación y de la supervisión,* una cuestión sobre la que advertimos hace más de veinte años.

CAMINO VIDAL FUEYO

La historia del constitucionalismo está ligada a las declaraciones de derechos y a la elaboración de una dogmática jurídica que, con el nacimiento de la Constitución normativa, nos ha conducido a un razonable sistema de protección de derechos fundamentales. En este marco, creo que el reconocimiento del derecho a la protección de datos personales, el *habeas data*, como derecho fundamental autónomo, es un paso imprescindible para una mayor garantía y protección de la privacidad, por diversas razones: en primer lugar, como consecuencia de la especial fuerza vinculante que deriva de su reconocimiento constitucional y que lo convierte en un derecho que obliga directamente a todos los poderes públicos; en segundo término, debido a la doble dimensión de los derechos fundamentales, que no sólo son derechos subjetivos, esto es, intereses jurídicos protegidos que podemos hacer valer ante los tribunales de justicia, sino también elementos objetivos, esenciales, del orden constitucional. Esto último nos lleva a concluir que la configuración de la protección de datos personales como derecho fundamental resulta imprescindible, pues de su reconocimiento no sólo se desprende la obligación de los poderes públicos de no lesionar este ámbito de privacidad de los ciudadanos, sino también la obligación positiva de contribuir a la efectividad de los mismos, incluso cuando no exista una pretensión subjetiva por parte del ciudadano, tarea que compete especialmente al legislador.

Asimismo, las nuevas tecnologías, en su concepción más amplia, constituyen un importante instrumento de poder en manos de particulares, por lo que la configuración del *habeas data* como derecho fundamental amplía el circulo de situaciones que dan sentido a la teoría de la *Drittwirkung* (a la eficacia jurídica directa

de los derechos fundamentales frente a los particulares), poniendo de relieve importantes contradicciones, pues las nuevas tecnologías, en su sentido más amplio, nacen como un espacio de libertad ajeno a toda autoridad estatal y, sin embargo, fuertes empresas de titularidad privada las monopolizan, dejando al sujeto individual inerme ante flagrantes injerencias en su ámbito de privacidad, particularmente en aspectos conectados a sus datos de carácter personal.

Por ello, y conectando con la segunda parte de la pregunta, relativa a las posibilidades con las que cuentan el Estado y el Derecho para hacer frente a amenazas de ese tipo, todo apunta a que la línea que se está siguiendo desde la Unión Europea, estableciendo una ordenación jurídica vinculante y homogénea a nivel europeo [Reglamento (UE) 2016/679, (RGPD)], es una vía adecuada para desarrollar el derecho fundamental a la protección de datos, estableciendo garantías y, a la vez, facilitando la circulación de los datos personales en el seno de la Unión, creando un espacio común de garantía del derecho.

Sería ingenuo atribuirle al Derecho facultades taumatúrgicas para hacer frente a todas las amenazas que para la intimidad y la vida privada de las personas se derivan de los avances tecnológicos, pero también sería irresponsable no utilizar las normas jurídicas para encauzar algunos de estos problemas y para evitar los peores riesgos. Gracias a la intervención del Derecho, la protección de datos personales descansa sobre una serie de reglas y de principios esenciales, cuyo estricto cumplimiento resulta una garantía y cuya vulneración conlleva la correspondiente sanción legalmente establecida.

Así, tanto la nueva normativa comunitaria, como la española, recogen una serie de normas vinculadas a unos principios que configuran las condiciones básicas para que los datos personales puedan ser tratados, tales como los principios de licitud, lealtad y transparencia del tratamiento, con el objeto de que no se puedan recoger datos de forma fraudulenta o ilícita y el titular esté informado en todo momento de su registro y tratamiento; el principio de limitación de la finalidad, que ha de ser determinada, explícita y legítima, permitiendo el control del uso que se hará de los mismos; el principio de minimización, de tal manera que los datos sean adecuados, pertinentes y no excesivos en relación con la finalidad para la que son tratados, también conocido como principio de «privacidad por defecto» (*privacy by default*), consistente en que se reduzca a los indispensables el número de datos personales tratados; el principio de exactitud, que exige que los datos estén al día y sean fiables; el principio de conservación de los datos, debiendo cancelarse cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos; el principio de integridad y confidencialidad, que evita un tratamiento no autorizado o ilícito aplicando las medidas técnicas u organizativas adecuadas, etc.

El RGPD introduce además el principio de responsabilidad proactiva que, con carácter general, implica que es el responsable del fichero el que tiene que aplicar «las medidas técnicas y organizativas apropiadas» a fin de garantizar y poder demostrar que el tratamiento cumple con la normativa de protección de

datos y que se tratan los datos personales de un modo lícito y seguro (art. 24.1 RGPD). Por otro lado, se exige cumplir con el principio de «privacidad desde el diseño» (*privacy by design*), que supone la obligación del responsable de desarrollar las medidas de protección de dichos datos (tanto técnicas como organizativas), con carácter previo al tratamiento de datos personales que se quiere realizar.

Todo ello me lleva a concluir, dando respuesta a la pregunta formulada, que el Derecho ofrece importantes mecanismos de defensa y garantía de este derecho y establece las pautas que han de seguir los poderes públicos para asegurar su plena eficacia.

3. *En el proceso de reconocimiento y determinación de este derecho fundamental han intervenido actores nacionales e internacionales. En este sentido ¿cree que el derecho a la protección de datos puede considerarse un ejemplo de derecho construido en un contexto de integración supranacional e incluso de globalización para hacer frente precisamente a una amenaza transnacional? ¿Qué balance haría de tal proceso?*

LORENZO COTINO HUESO

Ciertamente el reconocimiento del derecho de protección de datos es una atractiva historia sobre el reconocimiento inicial, construcción y evolución de un derecho fundamental y de la interactuación de un nuevo derecho con el régimen supranacional, constitucional y legal. Ello ha sido así especialmente en Europa, aunque también en el ámbito internacional y comparado.

En modo alguno puede preverse una seria regulación mundial de la privacidad y protección de datos. Sólo se han dado algunos impulsos desde Naciones Unidas tras los escándalos de Snowden. En algunas zonas la protección de datos es pírrica o ni se la espera (Asia, África) o bien hay palmarias diferencias con los niveles de la UE. Hay grandes asimetrías en materia de privacidad y protección de datos en las distintas regiones del mundo. Todo hace presagiar que lo mismo va a suceder con la inteligencia artificial.

Es muy interesante la evolución de la privacidad en Norteamérica a lo largo del siglo XX, siempre con una idiosincrasia propia con caminos bastante divergentes de Europa. Tras una visión de la privacidad esencialmente negativa en la primera mitad del XX también allí se ha ido reconociendo capacidad de control y deberes y obligaciones, al igual que asumiendo responsabilidades en la materia por instituciones especializadas para garantizar el cumplimiento de nuevos deberes, la *Federal Trade Commission* y la *Federal Communications Commission*. La diferente protección en EEUU de la privacidad y la protección de datos no siempre implica, como pensamos en Europa, una menor protección. En cualquier caso, siempre hay un importante contraste normativo que lleva por lo general a las empresas europeas a una desventaja competitiva con las de EEUU.

En Iberoamérica al inicio hubo interesantes aportaciones. No obstante, en buena medida su protección de datos ha quedado lastrada por muchos motivos. Entre ellos, se da cierta hibridez por algunos compromisos internacionales y comerciales con Estados Unidos y la influencia de su modelo. Tampoco ha sido allí positiva una mala emulación tanto de las leyes como los peores elementos del modelo de protección de datos en España, que posiblemente no ha sido el mejor ejemplo que deberían haber seguido. Igualmente, en Iberoamérica el derecho (fundamental) de acceso a la información pública y la transparencia se han anticipado a las leyes de protección de datos que, por lo general, han sido posteriores. A diferencia de lo que ha sucedido en Europa y particularmente en España, la transparencia ha tenido un peso cultural y normativo mayor que la privacidad.

Sin perjuicio de la situación mundial y regional internacional, en cualquier caso es incuestionable que en materia de protección de datos Europa, y en particular la UE, constituyen un referente y liderazgo mundial. Así, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981 (reformado en 2018) constituyó un hito que fue casi en paralelo con la famosa sentencia del censo del Tribunal Constitucional Alemán de 1983. Ambos supusieron un auténtico *pistoletazo* para una carrera para el reconocimiento jurisprudencial, legal y constitucional. Así tanto en el ámbito del Consejo de Europa (TEDH en el caso Leander, de 26 de marzo de 1987), como especialmente de la UE (Directiva 95/46/CE o, para las comunicaciones, la Directiva 2002/58/CE; reconocimiento en los tratados en 1997; la STJUE de 20 de mayo de 2003, caso Österreichischer Rundfunk; y la Carta de Derechos Fundamentales de la UE desde 2000) que ha culminado con el RGPD. Y cada Estado miembro ha tenido su propia evolución legal, constitucional y jurisprudencial.

El derecho de protección de datos ha ido tomando forma como una melodía con muchos actores, no siempre acompasada y armónica. Sin embargo, el resultado en Europa ha sido una maya jurídico-normativa bastante tupida que ha distinguido especialmente a la UE respecto de otras regiones del mundo que en ocasiones han quedado muy retrasadas y con un nivel de protección en modo alguno equiparable.

El RGPD de protección de datos empezó a elaborarse en 2012, en vigor desde 2016 y es aplicable desde 2018. El proceso de aprobación bajo las mayores presiones y dificultades muestra la gran relevancia del mismo y que se trata de una de las más ambiciosas normas en la historia de la UE. El resultado sin duda constituye un antes y un después en la acción normativa de la UE respecto de los derechos fundamentales. La dogmática, jurisprudencia y normativa de los estados miembros tiene que hacer importantes esfuerzos para *digerir* una regulación supranacional tan exhaustiva de un derecho fundamental, además tan importante económica, política, tecnológica y socialmente. Aunque se trate de un reglamento con efecto directo bien es cierto que concede un importante margen y se dan múltiples llamadas al legislador nacional. No obstante, en muchos casos, la capacidad de actuación nacional se asemeja más al margen del mero desarrollo

reglamentario de una ley, como sucede con la Ley orgánica 3/2018. Y es muy posible que el TJUE con los años vaya limitando aún más las posibilidades de actuación de los Estados. El contenido del RGPD tiene tal calado que su desarrollo y aplicación requerirá lo menos de una década para que despliegue sus efectos. Reino Unido fue un obstáculo para la adopción del RGPD y su salida de la UE puede ser un estímulo para una interpretación más rigurosa que evite fenómenos de *dumping* dentro de la UE (como ha sucedido especialmente con Irlanda).

Desde el punto de vista global, la regulación europea implica un nivel muy alto de protección y ello sitúa en desventaja a la UE frente a otras regiones o países. Esta situación se ha intentado compensar con una regulación de las transferencias internacionales de datos facilitadas a países con un nivel equivalente de protección. Asimismo, el RGPD pugna por proyectar sus efectos en todo el mundo con un ambicioso ámbito territorial (art. 3) para quienes hagan perfilados de residentes de la Unión o presten servicios o vendan bienes en la Unión. Esta extraterritorialidad ya la anticipó el derecho al olvido en 2014 sometiendo a Google a la regulación europea, al menos en sus resultados en el territorio de la Unión (como ha delimitado la STJUE de 24 de septiembre de 2019 Google vs. CNIL). Todo parece indicar que la política de la UE en materia de inteligencia artificial va a intentar seguir la estela de lo sucedido con la protección de datos. Así, quiere marcar un territorio en el que se den mayores garantías (Inteligencia artificial *Made in Europe*) y muy posiblemente quienes quieran proyectar los efectos o comercializar los productos de la inteligencia artificial en la UE habrán de cumplir también el Derecho de la Unión fuera de la UE. En esta misma dirección, el TJUE sigue siendo muy exigente respecto de los acuerdos de privacidad y protección de datos con Estados Unidos, habiendo anulado en 2020 el *Privacy Shield* que sustituyó al también anulado Sa*fe Harbour*.

ROSARIO GARCÍA MAHAMUT

Sin duda, y solamente un enfoque supranacional del derecho a la protección de los datos es lo que ha permitido dotar de mayor efectividad a su contenido y sistema de protección en un continuo proceso de evolución. De hecho, afirmar que el RGPD *europeiza* el derecho a la protección de los datos personales constituye una rotunda «verdad a medias». Como es por todos conocido, la europeización del derecho a la protección de datos se lleva produciendo desde hace décadas, solo basta recordar el punto de inflexión normativa que supuso para los Estados miembros la Directiva 95/46/CE. Buena prueba de la necesidad de actuar globalmente es, precisamente, el paso cualitativo que da el RGPD cuyo objetivo homogeneizador quiebra de forma decidida el principio de territorialidad nacional y la funcionalidad de las autoridades competentes a la hora de aplicar el RGPD. Por ello soy de la opinión, como muchos colegas, de que esa ruptura del principio de territorialidad y sus distintos engarces al servicio del efecto de homogeneización

normativa, que aún estamos lejos de conseguir, constituyen la clave de bóveda sobre la que descansa una las mayores aportaciones del RGPD.

Independientemente de consideraciones puntuales y en profundidad sobre aspectos y retos concretos que deben ser abordados en el seno de la UE desde una perspectiva absolutamente multidisciplinar, a mi juicio, en términos generales, el balance es tan bueno como desconsolador por los innumerables retos que se siguen cerniendo sobre una realidad que cruza fronteras y una regulación comunitaria que trata de alcanzarlos, pero donde siempre se abre una espita en la que la ponderación de derechos nos sitúa en una zona de conflicto jurídico constante, cuando no nos precipita a la oscuridad normativa más desoladora por la propia fragmentación jurídica europea y la red mundial de datos en continuo movimiento.

El RGPD, a no dudarlo, da un paso al frente y decidido en la configuración y garantías del derecho a la protección de datos, además de mejorar y apuntalar los distintos aspectos del ejercicio de un derecho que permea transversalmente tanto el ejercicio de otros derechos constitucionales como a los ordenamientos jurídicos de los distintos Estados miembros en la UE. De ahí que no podamos obviar el cambio de paradigma que se ha impuesto en la dogmática de los derechos fundamentales.

No obstante, ojalá todo se pudiera reconducir al RGPD. Muy lejos de esa realidad tenemos diversos sectores del ordenamiento jurídico afectados por la duda teórica. Pensemos, por ejemplo, como la Directiva 680/2016 de protección de datos en el ámbito penal no ha sido transpuesta en nuestro ordenamiento de forma sistémica y como, sin embargo, se conecta con otras realidades tales como la gestión de las fronteras y la seguridad nacional y la consiguiente apuesta comunitaria destinada a lograr la interoperabilidad de los sistemas de información de la UE para mejorar la gestión de las fronteras, la migración y la seguridad interior con el objetivo de solucionar las deficiencias estructurales relacionadas con tales sistemas y así garantizar que los guardias de fronteras, las autoridades aduaneras, los agentes de policía y las autoridades judiciales tengan a su disposición la información necesaria.

Pero a más, solo pensamos en vía unidireccional cuando hablamos de protección de datos, mientras que la realidad normativa es diversa y asombrosamente compleja. Tenemos un RGPD, pero también una normativa comunitaria dispersa y difusa que afectando a la protección de los datos personales impacta en todos los ámbitos de la existencia humana; y, sin embargo, las tradicionales disciplinas jurídicas no pueden con solvencia abordar la interpretación y aplicación de la norma frente a los diversos conflictos jurídicos que se plantean al escapar de una metodología jurídica tradicionalmente compartimentada. Pensemos, por ejemplo, en el difuso régimen jurídico de protección de datos en el SECA que lleva aparejado la más absoluta de las inseguridades jurídicas. Desde la aplicación del RGPD, pasando por sus excepciones con la aplicación de Directiva 680/2016 de protección de datos en el ámbito penal —a día de hoy no transpuesta por parte de España— sin pasar por alto la implementación del Reglamento 2018/1725

para el tratamiento de datos personales que realizan todo el conjunto de instituciones, órganos y organismos de la UE.

En íntima conexión con ello, recalemos por un momento en los Reglamentos de interoperabilidad 817/2019 y 818/2019. En fin, la complejidad del marco normativo en diversos ámbitos jurídicos inextricablemente unidos es inmenso, está integrado —como en su momento señaló el Supervisor Europeo de Protección de Datos— por demasiados «elementos móviles».

Si tuviera que resumir en pocas palabras el balance del proceso diría que hemos avanzado increíblemente, pero queda un inmenso camino por recorrer.

PABLO LUCAS MURILLO DE LA CUEVA

Desde luego, es fruto de la circulación de las ideas propia de los tiempos presentes. He mencionado antes tres coincidencias producidas en el año 2000 que no son casuales. El Tribunal Constitucional, cuando falla la sentencia 292/2000, ya conoce tanto los pronunciamientos del Tribunal Europeo de Derechos Humanos como los trabajos preparatorios de la Carta de los Derechos Fundamentales aprobada pocos días después por la cumbre de Jefes de Estado y de Gobierno de Niza de la Unión Europea. Y la Carta se nutre de la jurisprudencia de Estrasburgo y, también, de la experiencia surgida bajo la Directiva 95/46/CE. A su vez, esta última y las legislaciones nacionales dictadas a esas alturas son todas tributarias del Convenio n.º 108 del Consejo de Europa. En fin, este último se sirve de estudios y experiencias surgidas en los países democráticos europeos. Si miramos a acontecimientos más recientes, es evidente la relación de los difíciles trabajos que han llevado al Reglamento (UE) 2016/679 con la jurisprudencia de Luxemburgo y Estrasburgo; y, a la vez, en el Protocolo 223 del Consejo de Europa que pone al día el Convenio 108, son visibles los elementos principales que aporta el Reglamento (UE) 2016/679.

Hoy en día, afortunadamente, hay una comunicación intensa y fluida entre los múltiples niveles institucionales, económicos, sociales y académicos implicados y entre quienes, desde diversas posiciones, se ocupan de aplicar y de analizar el Derecho de la Protección de Datos. La jurisprudencia de Estrasburgo y la emanada del Tribunal de Justicia son referencias comunes no sólo para aplicar conforme a ellas el régimen jurídico establecido por la Unión Europea y sus complementos nacionales y las exigencias del Convenio de Roma sino, también, para buscar en su seno los principios desde los que resolver los nuevos problemas que van apareciendo cada día —la realidad de los datos personales es extraordinariamente dinámica— y para los que no hay una previsión normativa específica. Se suele hablar del diálogo entre tribunales para explicar la relación que se establece entre los jueces nacionales y el Tribunal de Justicia o el Tribunal Europeo de Derechos Humanos. Pues bien, en este campo creo que hay una conversación permanente entre los integrantes del amplio conjunto de sujetos interesados por la

protección de los datos personales basada en el común empeño de avanzar en la salvaguardia de esa parcela de la personalidad en que consiste la autodeterminación informativa.

Será especialmente importante mantenerla para profundizar en uno de los aspectos que incorpora el Reglamento y que está previsto también en el Protocolo 223 del Consejo de Europa. Se trata del derecho del afectado a ser informado, a conocer la lógica —dicen los artículos 13.2 f). 14.2 g) y 15.1 h) del primero y explica su considerando (63)— o el razonamiento —dice el segundo, en su artículo 9.1 c)— implícitos en todo tratamiento de datos personales. Se trata, pues, de ampliar el derecho más allá del conocimiento de los fines para los que se va utilizar de manera que se extienda a los criterios que lo presiden y que pueden llevar a una u otra caracterización de los afectados y a atribuirles un determinado perfil.

MANUEL MEDINA GUERRERO

No cabe la menor duda de que el derecho, tal y como lo concebimos actualmente, es fruto del proceso de integración normativa experimentado en la UE a raíz, fundamentalmente, de la Directiva 95/46/EC. Directiva que cedió el paso al RGPD cuando se constató que era necesario avanzar en la homogeneización normativa entre los países miembros de la Unión.

Por el contrario, no creo que la conformación de nuestro derecho se haya producido en un contexto de mundialización, pues, al fin y al cabo, y salvando contadas excepciones (Canadá, por ejemplo), el nivel de protección que se brinda a este derecho en la generalidad de los Estados se halla muy a la zaga del que se dispensa en el marco de la UE. Sí es posible apreciar un efecto irradiación de la «cultura europea» en materia de protección de datos a otros países, como sucede en la esfera latinoamericana gracias —entre otros factores— a la importante tarea realizada al respecto por la AEPD.

La menor tutela generalmente existente en terceros países explica por qué ya la Directiva 95/46/EC dedicara el Capítulo IV a asegurar que el derecho a la protección de datos personales de los ciudadanos europeos no se viera comprometido cuando tales datos se envían al exterior; régimen de transferencia de datos personales a terceros países que, en lo esencial, se mantiene en el RGPD. Para decirlo en términos sumamente sintéticos, dos son las vías que permiten salvaguardar la legitimidad de estas transferencias internacionales. Por una parte, el artículo 45 RGPD contempla la existencia de una «decisión de adecuación» de la Comisión Europea que declare que el país destinatario garantiza un «nivel de protección adecuado»; mientras que, por otro lado, el artículo 46.1 RGPD autoriza que se transmitan datos personales a terceros países si se ofrecen «*garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas*».

La experiencia de estos mecanismos de transferencias de datos ha tenido una turbulenta trayectoria en relación con los Estados Unidos. Como es sabido, la

Decisión de «Puerto Seguro» (Decisión 2000/520/CE) fue declarada inválida por la STJUE de 6 de octubre de 2015 [caso *Schrems* (C-362/14)]; y seriamente afectado ha resultado el «Escudo de Privacidad» [Decisión de Ejecución (UE) 2016/2015 de la Comisión, de 12 de julio de 2016], que vino a reemplazar a aquélla, con motivo de la STJUE de 16 de julio de 2020 [caso *Schrems 2*].

ARTEMI RALLO LOMBARTE

Sin duda alguna, sí. Así lo hemos defendido muy recientemente («El nuevo derecho de protección de datos», *Revista Española de Derecho Constitucional*, 116, 2019, pp. 47-74), cuando, para referirnos al nuevo derecho de protección de datos, hablamos de la «abducción de un derecho constitucional convertido en un derecho exclusivamente europeo».

El RGPD y la LOPDGDD ofrecen hoy un marco normativo, europeo y nacional, de protección de datos que es el resultado de una construcción vertical descendente cuyo origen remoto reside en instrumentos internacionales como el Convenio 108 del Consejo de Europa de 1981 y las Directrices de la OCDE de 1980 y que adquirió plenitud con la Directiva 95/46/CE y el art. 8 CDFUE. Este nuevo derecho de protección de datos implica una severa mutación en el sistema constitucional de fuentes al producirse una auténtica abducción del derecho constitucional que se ha convertido en derecho exclusivamente europeo y sometido a la excluyente normación de la Unión Europea y a la fijación de canon hermenéutico por el TJUE. Un efecto adicional y colateral de este impacto constitucional radica en la devaluación de la posición constitucional de la ley orgánica que queda marginalmente limitada a garantizar la aplicación efectiva del RGPD.

Este *nuevo Derecho* de protección de datos constituye un marco normativo multinivel en el que interaccionan normas europeas y nacionales. No estamos ante un *nuevo derecho* de protección de datos pero pudiera parecerlo a la vista de los elementos que hacen reconocible este derecho y el sistema de garantías que lo ampara. El fundamento constitucional del derecho fundamental de protección de datos se ha desplazado del ámbito nacional al europeo y, sobre este último anclaje, se ha normativizado un derecho fundamental homogéneo en toda la Unión Europea a través de un RGPD cuya base jurídico-constitucional deriva, de forma única y exclusiva, del art. 8 CDFUE (aunque convive cómodamente con las tradiciones constitucionales de los Estados miembros que han ido progresivamente forjando este derecho fundamental de protección de datos). Los elementos definitorios del derecho consagrado en el art. 8 CDFUE se asimilan sin dificultad a los rasgos definitorios del contenido esencial del derecho fundamental de protección de datos consolidado progresivamente en el ámbito dogmático y por las jurisdicciones constitucionales nacionales. Pero el actor más sacrificado por este nuevo modelo ha sido el legislador nacional.

La protección de datos no nació como un derecho y en muchas latitudes (por ejmpleo, USA) sigue negándosele tal naturaleza pero resulta incuestionable su consolidación actual como derecho fundamental tras protagonizar una historia europea de éxito. Los primeros documentos internacionales se limitaban a caracterizar la protección de datos como una estrategia transnacional para facilitar el flujo internacional de datos personales y promover el desarrollo global de la economía de mercado. La propia Directiva 95/46/CE sustentaba su base legal en la libertad de circulación y en la proscripción de obstáculos que impidieran tal fin como objetivo esencial para el mercado interior. En fin, la protección de datos constituía un objetivo secundario frente a un fin principal. Pero otras iniciativas de carácter nacional forjaron un emergente derecho de protección de datos que acabaría consolidándose legislativamente e, incluso, en el plano constitucional. No es de extrañar que el constituyente portugués (1976) y el español (1978) constitucionalizaran este emergente fenómeno de la *informática* y que, en los albores del nuevo milenio, la CDFUE aprobada en Niza en 2000 consagrara el derecho fundamental de toda persona a la protección de datos personales (art. 8).

El RGPD desarrolla, de forma completa y exhaustiva el art. 8 CDFUE, excluyendo cualquier intervención estatal dirigida a regular este derecho fundamental. Cualquier debate en torno a la primacía del art. 8 CDFUE sobre el art. 18.4 CE adquirirá una mera relevancia teórica alejada de controversias reales por cuanto la CDFUE se concibe como una garantía de mínimos. La convivencia del art. 8 CDFUE y del art. 18.4 CE está pacíficamente garantizada por vía hermenéutica ya que el derecho fundamental garantizado por el 18.4 CE va a ser directa y principalmente regulado por el RGPD desplazándose el canon de protección del derecho fundamental a la interpretación que del art. 8 CDFUE haga el TJUE. Por su propia naturaleza, el RGPD resulta de alcance general y directamente aplicable sin que quepa imaginar un nivel básico de protección otorgado por la normativa europea ampliable por garantías adicionales provenientes del Derecho interno. El derecho de protección de datos quedará garantizado conforme a lo previsto por el RGPD y, por vía prejudicial, por la jurisdicción europea sin que las instancias jurisdiccionales o legislativas nacionales puedan modificar la conformación de este derecho europeo.

LUCRECIO REBOLLO DELGADO

Desde mediados de los años sesenta se constata en Europa la importancia del uso de las telecomunicaciones, así como la necesidad de una legislación que unifique pretensiones, y especialmente, que ofrezca un conjunto de medios de protección de los derechos y libertades fundamentales. Afortunadamente, a este ámbito de actuación, tanto del Consejo de Europa, como de la Unión Europea, se le pueden formular pocos reproches, y conviene destacar que si bien es frecuente que la legislación genérica de la Unión Europea suele ser de mínimos, en la

protección de datos, puede afirmarse con rotundidad que ha supuesto que los Estados miembros hayan ido elevando progresivamente su nivel de protección, produciendo un efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos.

El Reglamento General de Protección de Datos de la UE de 2016 (en adelante RGPD) viene a culminar una necesidad a nivel europeo, y a perfeccionar el camino iniciado por el Convenio 108 de 1981, y la Directiva 95/46/CE. Se pretende hacer con una mayor efectividad, con más decisión. Por ello se varía el tipo normativo utilizado, que pasa de ser Directiva a Reglamento. De esta circunstancia hay que extraer una clara intencionalidad del legislador de la Unión, que no es otra que la de establecer una regulación homogénea en su ámbito de vigencia territorial, que elimine en el mayor grado posible las singularidades o variaciones en el cumplimiento de lo nuclear de la normativa por parte de los Estados miembros. Al eliminar la necesaria intervención de los Estados en la creación normativa básica se está buscando la inmediatez en la consecución de sus finalidades, a la vez que estableciendo un sustrato jurídico común a todos los Estados miembros. No obstante, el RGPD utiliza de forma frecuente contenidos muy abiertos, o incluso claras remisiones, ya sean a los Estados miembros o a órganos de la Unión Europea, y especialmente a la Comisión.

Otro aspecto capital que viene a solventar el RGPD es la necesidad de adecuar la normativa a los avances tecnológicos producidos. Esta es una circunstancia constante en esta área del derecho, que necesita dar soluciones jurídicas de forma rápida a las nuevas posibilidades técnicas, y singularmente solventar los problemas jurídicos que ellas originan, o esencialmente, proteger al ciudadano ante posibles vulneraciones de derechos y libertades fundamentales.

Una tercera causa que justifica la nueva regulación proviene de los sustantivos cambios que introduce el Tratado de Lisboa. Liquida la estructura de pilares de la Unión, lo que supone que ámbitos que no estaban afectos por la Directiva 95/46/CE y que por tanto no estaban incluidos en una regulación específica, pasan ahora a estarlo, así ocurre con las materias de ámbito policial, judicial, la política exterior y la seguridad común, así como los tratamientos de datos personales que tengan por objeto la defensa, o la seguridad pública o del Estado.

Un cuarto aspecto que viene a solventar el Reglamento con respecto a la Directiva 95/46/CE es el punto de mira en que se concreta la protección. La Directiva fijaba como objetivo de su contenido y elemento esencial en la aplicabilidad de la misma la radicación de los datos. Producto de la globalización, ello suponía una inmensa puerta abierta, que dejaba vacía de contenido sus postulados en múltiples ocasiones. Un portillo jurídico en toda regla, y que venía constituyendo una preocupación sustantiva de cara a la protección de los derechos de los usuarios. Para paliar esta deficiencia el Reglamento establece como objetivo de su regulación partir de la ubicación del interesado y dónde se realiza el tratamiento, singularmente la radicación del responsable del mismo, como elemento delimitador básico para la aplicabilidad y plena vigencia de la norma.

Por último, existe una justificación del nuevo Reglamento que entronca con las nuevas pretensiones conformadoras y sustentadoras de la Unión Europea. No existe la menor duda de que la construcción de ésta tiene un claro origen mercantil, pero desde el Acta Única de 1986 se ha pretendido hacer virar la Unión a un conjunto más abierto, que incluya todas las necesidades del ciudadano, siendo una parcela esencial en ello el reconocimiento y garantía de los derechos y libertades fundamentales. Teniendo los Estados miembros un alto grado de reconocimiento y garantía de los derechos y libertades, la Unión Europea ha querido ponerse a la cabeza de un área específica de éstos, la protección de datos de carácter personal. Ello se justifica en la necesidad del carácter supranacional de estas regulaciones, pero no debemos olvidar que también afecta a uno de los pilares básicos de la construcción europea, el libre tránsito de personas y mercancías por el espacio común.

En resumen, el balance tiene que ser obligatoriamente positivo, y puede afirmarse con rotundidad que la UE ha respondido a las necesidades de regulación y de garantía efectiva de los derechos y libertades fundamentales ante los nuevos desafíos tecnológicos. Pero como hemos manifestado, esta es una actividad siempre inacabada, en constante desarrollo, dado que cada día se producen nuevos retos, nuevas posibilidades, que exigen una adecuación y puesta en práctica de soluciones constantes.

ANTONIO TRONCOSO REIGADA

El derecho a la protección de datos personales, como señala la pregunta, se ha construido en un contexto de integración supranacional. Las tres leyes de protección de datos aprobadas en España nacen de un impulso europeo: la LORTAD, del Convenio 108 del Consejo de Europa, del Acuerdo de Schengen y de la Propuesta de Directiva; la LOPD, de la Directiva 95/46/CE; y la LOPDGDD, del RGPD. Pocos derechos son tan importantes para la construcción europea y para hacer viable ese espacio común que hoy representa la Unión Europea como el derecho fundamental a la protección de datos personales. Si el objetivo clásico de la Unión Europea era la libre circulación de personas, mercancías y capitales, y, por tanto, de datos personales, esto movimiento solo era posible si los países que la componen disponían de un modelo de protección de datos personales homogéneo que permita el intercambio de información.

Sin embargo, las divergencias en la protección de los datos personales entre los Estados miembros de la Unión Europea en el marco de la Directiva 95/46/CE eran demasiado grandes. Esto obedecía fundamentalmente a tres razones: en primer lugar, el margen de maniobra que dejaba la propia Directiva como derecho derivado institucional y sus abundantes cláusulas abiertas —*open-ended principles*— que admitían una transposición diferente en la legislación de los distintos Estados; en segundo lugar, la inadecuada transposición de la Directiva 95/46/CE

por la propia legislación de los Estados miembros que había incumplido sus exigencias y había sobrepasado sus límites; en tercer lugar; la disparidad en la capacidad coercitiva de las autoridades de control —o una distinta voluntad de ejercer los instrumentos coercitivos— y la deficiente interpretación y aplicación que llevan a cabo las autoridades de control y los órganos jurisdiccionales en los diferentes Estados de los mismos principios y derechos recogidos en la Directiva ante similares supuestos de hecho. Estas diferencias en la protección de los datos personales entre los Estados miembros obstaculizaban el mercado interior, dificultando el ejercicio de actividades económicas a escala comunitaria y falseaban la competencia. Además, la ausencia de protección equivalente afectaba también a la eficacia del derecho fundamental a la protección de datos personales de los ciudadanos europeos.

La aprobación del Tratado de Lisboa reforzó la base jurídica en la Unión Europea para aprobar una normativa en virtud del reconocimiento de un derecho fundamental a la protección de datos personales en el art. 8 de la Carta, y permite extender la vigencia del derecho europeo de protección de datos personales al ámbito del antiguo tercer pilar. El RGPD es el marco jurídico coherente y homogéneo de protección de datos que suprime las incongruencias entre los Estados miembros y reduce el margen de elección tanto de los legisladores nacionales como de las autoridades de control, desplazando la mayor parte de la legislación de los Estados y facilitando una política más integradora en la Unión Europea en este ámbito. Al mismo tiempo, el RGPD permite una protección más efectiva de los ciudadanos europeos frente a los tratamientos de datos a escala internacional, que puede lograrse mejor a nivel de la Unión.

Hay que recordar que el RGPD, al igual que la Directiva 95/46/CE, no tiene como único objetivo la protección de las personas físicas en lo que respecta al tratamiento de datos personales sino también favorecer la libre circulación de estos datos de manera que no sea restringida ni prohibida por la protección de datos personales. El RGPD, siguiendo los objetivos de este proceso de integración supranacional, tiene la voluntad de contribuir a la creación de un mercado digital europeo que favorezca el crecimiento de la actividad económica y mejore la competitividad de las empresas europeas, lo que requiere la adopción de decisiones encaminadas a facilitar la libre circulación de datos personales en la Unión Europea. No hay que olvidar que la decisión de promover la elaboración de un nuevo RGPD se adopta por la Comisión en el año 2012 también en un contexto de fuerte crisis económica, por lo menos en España. Este es también uno de los objetivos de la Directiva 2016/680, que supone un importante avance en la regulación de la protección de datos personales en un ámbito como el policial y el judicial que hasta el Tratado de Lisboa se movía en los terrenos de la cooperación y no de la integración. De esta forma, la Directiva 2016/680, al mismo tiempo que pretende llevar a cabo una primera armonización normativa en protección de datos personales en un ámbito que hasta ahora pertenecía a la soberanía de los Estados y que estaba regulado por la Decisión Marco 2008/977/JAI del Consejo,

tiene también la voluntad decidida de facilitar la compartición de información policial y judicial, mejorando la eficacia policial ante un desafío terrorista que no tiene en cuenta las fronteras nacionales y cuyos autores se mueven libremente en el espacio *Schengen*. Por tanto, la libre circulación de datos personales para favorecer el mercado digital y para permitir el intercambio de información policial y judicial es uno de los desafíos que justifica que la Unión Europea haya impulsado este nuevo marco normativo europeo al mismo nivel —al menos— que la tutela del derecho fundamental a la protección de datos personales.

Para lograr este objeto de favorecer la libre circulación de los datos, la Unión Europea ha establecido una regulación común de protección de datos personales, a través de la aprobación de una norma de derecho derivado institucional como es el Reglamento, que a diferencia de la Directiva 95/46/CE, es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro, lo que permite superar la fragmentación de las legislaciones de protección de datos existente en los diferentes países de la Unión Europea durante el periodo de vigencia de esa Directiva. Existía un convencimiento en la industria y en los mercados de que la diferente transposición de la Directiva 95/46/CE por los Estados miembros había dificultado la comercialización de productos y servicios y el desarrollo de políticas de privacidad paneuropeas, al obligar a las empresas a adaptar sus productos a las distintas extensiones normativas nacionales. Esta situación, además de suponer un incremento de costes, representaba un límite a la competencia y al funcionamiento del mercado interior en la Unión Europea, encontrándose muchas empresas europeas en una situación de desventaja en el mercado. Por ello, la aprobación del RGPD, que establece normas comunes de protección de datos personales y que mejora sustancialmente la armonización normativa en este punto, favorece la competitividad de las empresas y la investigación, lo que permite la creación en Europa de un sector industrial y empresarial fuerte también en el ámbito de la economía digital, que pueda competir con otros ámbitos geográficos fuera de la Unión Europea como EE.UU. y Asia-Pacífico.

En esta dirección hay que subrayar que la Comisión Europea está elaborando una comunicación sobre «Una estrategia europea para los datos» donde se plantea la creación de un espacio único para los datos mediante la agrupación e interconexión de las plataformas virtuales, públicas y privadas, de almacenaje de los veintisiete Estados miembros. Si el origen de la Unión Europea está en el establecimiento de un mercado común del carbón y del acero (CECA)- y de la energía atómica (Euratom)-, la Unión Europea pretende la creación de un «espacio común europeo» de datos. La materia prima por excelencia del siglo XXI son los datos de los ciudadanos, esenciales para el crecimiento económico, para la innovación y para la investigación sanitaria. Europa no puede depender completamente de proveedores no europeos para el almacenamiento y procesamiento de la información de ciudadanos europeos, algo que entraña graves riesgos tanto para los derechos de los ciudadanos europeos —en especial

para la protección de datos personales— como para la soberanía de los Estados y la posición de la Unión Europea en el actual contexto geopolítico. Hay que apostar porque Europa entre de lleno en la economía digital siguiendo un modelo más garantista para los derechos fundamentales, a diferencia de otros modelos existentes en China —haciendo valer la protección de datos como derecho frente al Estado o frente a empresas-Estado— o en EEUU —como derecho frente a las corporaciones privadas y también frente al Estado—. Sin embargo, tampoco se puede defender un modelo de máximos, excesivamente riguroso, que dificulte mucho su implantación, lo que tendría como consecuencia paradójica e indeseada a medio plazo una reducción de la protección de datos personales de los ciudadanos europeos.

El RGPD facilita las transferencias de datos personales a terceros países y a organizaciones internacionales si existen garantías adecuadas recogidas en instrumentos de autorregulación como normas corporativas vinculantes, códigos de conducta o mecanismos de certificación. Esta previsión permite a las empresas europeas intercambiar datos personales fuera de la Unión Europea y competir en mercados distintos del europeo. Esta apuesta decidida del legislador europeo por las herramientas de autorregulación también en las transferencias internacionales de datos personales beneficia el equilibrio entre las diferentes visiones sobre la protección de datos personales a nivel internacional, lo que también favorece el diálogo económico trasatlántico y con otras regiones, ampliando las posibilidades de crecimiento económico y de creación de empleo. Por tanto, la mayor armonización europea en el ámbito de la protección de datos producida por la sustitución de la Directiva 95/46/CE por el RGPD, así como la introducción en este último de elementos procedentes de la autorregulación son dos instrumentos que, aunque aparentemente pueden parecer contradictorios —no lo son en realidad—, favorecen la libre circulación de los datos personales en la Unión Europea y fuera de ella.

Si la protección de datos personales es un elemento esencial para la construcción europea y para la integración supranacional, lo es aún más en el contexto de la globalización. Durante los últimos años se ha hecho más evidente la necesidad de garantizar la privacidad en un mundo sin fronteras, especialmente desde la aparición de Internet, y caracterizado por continuas transferencias internacionales de datos personales. No nos referimos únicamente al intercambio transfronterizo de datos derivado del incremento de las relaciones económicas y comerciales con otros países, especialmente del área Asia-Pacífico sino a los tratamientos de la propia esfera personal o doméstica —motores de búsqueda, redes sociales, computación en nube— que se desarrollan por Internet a través de redes internacionales cuyos usuarios y proveedores de servicios se encuentran ubicados en países diferentes y donde el servidor informático se encuentra también en un tercer país. Ante una amenaza a los derechos de carácter transnacional, como señala la pregunta, cada vez es más complicado determinar la jurisdicción competente y la legislación aplicable y quien es el responsable del tratamiento. Por ese motivo, el

legislador europeo ha regulado acertadamente el ámbito territorial de aplicación del RGPD, resolviendo la problemática que plantean las corporaciones internacionales que ofrecen servicios de tratamiento de datos a ciudadanos europeos y que tienen su sede fuera de la Unión Europea. El RGPD establece una clara orientación hacia las personas, lo que obliga al responsable o al encargado del tratamiento que no se encuentre establecido en la Unión a aplicar el RGPD al tratamiento de datos personales de interesados que residan en la Unión cuando las actividades de tratamiento estén relacionadas con oferta de bienes o servicios a ciudadanos europeos o el control de su comportamiento en la medida en que tenga lugar en la Unión.

Sin embargo, en un entorno globalizado e interconectado con constantes flujos de información personal la normativa regional no siempre sirve para responder ante eventuales amenazas. El derecho a la protección de los datos personales no es real y efectivo con la mera aplicación de la normativa de la Unión Europea. Se muestra, así, de manera clara que la protección de los datos personales tiene una dimensión internacional de la que carecen otros derechos fundamentales y su tutela efectiva exige también una normativa internacional. Por ese motivo, es importante que se establezcan exigencias homogéneas de privacidad a nivel internacional, que superen las discrepancias existentes —por no decir los desequilibrios— entre la Unión Europea, Estados Unidos y el ámbito Asia-Pacífico y ofrezcan seguridad jurídica a todos los agentes —industria, sociedad civil, Administraciones Públicas, autoridades de control—. La aprobación de un Tratado internacional que establezca una normativa de protección de datos personales y unas reglas de supervisión a nivel internacional es algo imprescindible, lo que requiere alcanzar un equilibro entre las diferentes visiones sobre la protección de datos personales en los distintos continentes. Un primer paso en esta dirección fue la Resolución de Madrid de Estándares Internacionales sobre Protección de Datos Personales y Privacidad de 2009, un documento nacido del diálogo y de la búsqueda del consenso que trataba de integrar las sensibilidades presentes en los distintos continentes y que tenía por objeto «definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal» —art. 1—. Hay que destacar el papel que jugó el Director de la AEPD, Artemi Rallo, que tuvo la inteligencia y el liderazgo necesario que posibilitaron la aprobación de esta Resolución.

Asimismo hay que subrayar la importancia del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que desarrolló el art. 8 del CEDH y que fue el primer instrumento internacional vinculante en materia de protección de datos personales en los sectores público y privado, que señaló los elementos principales del contenido del derecho fundamental. El interés del Consejo de Europa por mantener el carácter abierto del Convenio 108, permitiendo la adhesión de países no europeos —en la actualidad hay ocho Estados no miembros del Consejo de Europa que han suscrito el Convenio 108— refuerza su

potencial carácter de estándar internacional, por lo que es relevante promover su ratificación por países no europeos que aprueben una legislación adecuada. En el año 2018 se ha adoptado un Protocolo Adicional que modifica el Convenio 108 —el llamado «Convenio 108 +»—, que aborda la protección de datos desde la perspectiva de la globalización y del incremento de la circulación de la información. Es importante destacar que la Unión Europea y el Consejo de Europa hayan impulsado al mismo tiempo un cambio en su normativa de protección de datos y que esté presente en ambos textos la vocación y la preocupación por ser compatibles y en ningún caso contradictorios.

Lógicamente, al hacer una valoración sobre el balance de este proceso, emerge el debate de fondo sobre el papel regulador —principal o subsidiario— de los Gobiernos en Internet y la necesidad de establecer un marco jurídico eficaz, no para limitar Internet, sino para asegurarse de que prospera sobre la base del respeto a la privacidad y a los derechos de las personas. Lógicamente, la vía que le interesa a la industria para la protección de los datos personales es la autorregulación y el papel subsidiario de los Gobiernos —que ha sido hasta ahora el modelo norteamericano—. Ya hemos señalado antes que el RGPD incorpora muchos instrumentos propios de la autorregulación que es una herramienta útil, sobre todo cuando falta una regulación jurídica en el ámbito internacional o nacional, en situaciones de gran complejidad técnica o ante la imposibilidad de llegar a todos los ámbitos a través de una actividad administrativa de inspección y control, pudiendo contribuir a la protección de los derechos del usuario. Sin embargo, que la autorregulación ha demostrado sus limitaciones —que el mercado tiene sus límites— es algo que se evidencia con la aproximación de los países iberoamericanos hacia el modelo europeo de protección de datos personales, que fue premiado con la declaración por parte de la Comisión Europea de que estos países garantizan un nivel adecuado de protección —Argentina, 2003; Uruguay, 2112—. La autorregulación no llega a garantizar con plenitud los derechos de los afectados por lo que hay que aplicar también en este ámbito la regulación, la supervisión y, en general, los instrumentos heterónomos. Sin perjuicio de la importancia de la autorregulación, los Estados democráticos y las entidades internacionales y supranacionales son los últimos garantes de los derechos de las personas y no deben renunciar a la regulación en Internet. El modelo europeo de protección de datos ha apostado por las herramientas normativas heterónomas, de ahí su fuerte asimetría con el modelo norteamericano. Hay que subrayar la importancia de la reciente STJUE, de 16 de julio de 2020 — As. *Facebook Ireland contra Schrems*-, que anula la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad UE-EE.UU (*Privacy Shield*) para las transferencias internacionales de datos a EEUU —que a su vez sustituía al modelo de Puerto Seguro, que también fue anulado por el TJUE en octubre de 2015— y que considera válida la Decisión 2010/87 de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, lo que pone de

manifiesto todavía la subsistencia de diferentes modelos de protección de datos personales a uno y otro lado del Atlántico y que dificulta las transferencias de datos personales.

CAMINO VIDAL FUEYO

Tal y como he expuesto en mi respuesta a las preguntas precedentes, considero que la regulación jurídica dirigida a la protección de los datos personales resulta necesaria, pero también soy consciente de la dificultad fáctica a la hora de regular una realidad, la digital, sin fronteras, ni contornos físicos y en muchos aspectos impermeable al control estatal. Por ello, la incidencia de las nuevas tecnologías en la privacidad de las personas refuerza la crisis de la noción clásica de soberanía y la correlativa necesidad de crear normas jurídicas internacionales vinculantes para los Estados, que sirvan de mecanismo de defensa de los derechos y libertades de todas las personas. La vigente Constitución española no es ajena a esta necesidad y habilita al Estado para integrarse en unidades políticas supraestatales con la consiguiente transferencia de competencias; incorpora al ordenamiento interno los tratados internacionales como fuente de Derecho, así como la cláusula de remisión, a efectos interpretativos, del art. 10.2 CE, que constituye un poderoso mecanismo para la integración de España en un estándar universal de reconocimiento y protección de derechos humanos.

Tal y como enfatiza Fernando Fernández-Miranda, este derecho, lejos de ser reconocido de forma global mediante normas internacionales vinculantes, está regulado y garantizado de manera muy desigual en los diferentes países y continentes. Así, por ejemplo, Estados Unidos y Europa ha seguido caminos diferentes y, en algunos aspectos, contrapuestos, debido a una diferente concepción del individuo frente al Estado. No obstante lo anterior, este experto sostiene que el reconocimiento del derecho a la protección de datos ha contado, en el ámbito internacional, con un denominador común que surge del célebre concepto anglosajón *the right to be let alone*, construido dogmáticamente ya en el año 1890 por Warren y Brandeis en su artículo «The Right to have privacy» (Harvard Law Review), asumido por los tribunales estadounidenses y que las legislaciones y jurisdicciones europeas desarrollaron adaptándolo a su particular perspectiva democrática y jurídica de la privacidad del individuo.

En el año 2020, es palmario que el riesgo relativo a la falta de control sobre la circulación y el uso de los datos personales se ha visto potenciado por la globalización, cuyo origen está vinculado, entre otros factores, precisamente a los avances informáticos y tecnológicos. Sin embargo, la magnitud del impacto de dichos riesgos no es percibida con el mismo recelo e inquietud en todas las jurisdicciones, por lo que nos encontramos ante una amenaza que, si bien afecta por igual a todo el territorio mundial, no es atajada de igual forma y con los mismos instrumentos jurídicos, siendo la Unión Europea el único ejemplo de regulación

homogénea para todos los estados miembros, a través de la entrada en vigor, el 25 de mayo de 2018, 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 sus datos personales y a la libre circulación de estos datos, que establece un nuevo y más riguroso estándar de protección de los datos personales atendiendo a nuevas circunstancias, principalmente al aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado. Esta regulación se ha erigido como modelo a seguir por algunos ordenamientos extracomunitarios, como está ocurriendo en Brasil, en México o en el Estado de California, que han legislado recientemente sus propias normas de privacidad inspirándose en el texto europeo. Asimismo, cada vez más grupos multinacionales con presencia en todo el mundo llevan a cabo el tratamiento de datos personales en el contexto de su actividad mercantil conforme a las disposiciones del RGPD, con independencia del país en el que se encuentre cada una de las empresas que lo conforman.

Sin duda el hecho de que a nivel comunitario se escogiera la figura del Reglamento para actualizar la normativa europea de protección de datos (hasta el año 2016 regulada en forma de Directiva) ha servido para homogeneizar las legislaciones nacionales y para ampliar el elenco de garantías con las que cuentan los ciudadanos, pues además de ver ampliadas las facultades y derechos que configuran el *habeas data*, cualquier ciudadano de un Estado miembro puede acudir a los tribunales nacionales e invocar directamente lo previsto en el Reglamento, sin necesidad de que existan previsiones nacionales al efecto. Ello no **es** óbice, como es lógico, para que los legisladores nacionales configuren también, por el calado y la complejidad de las reformas introducidas por el Reglamento, una regulación propia acorde a sus específicas necesidades.

En este sentido, el legislador español ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que, tal y como se desprende de su exposición de motivos, pretende desarrollar y complementar el RGPD, y aporta novedades tales como la regulación de los datos referidos a las personas fallecidas, al permitir por primera vez que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, con sujeción a las instrucciones del fallecido.

Se trata de una Ley Orgánica cuya valoración general es positiva, sin perjuicio de que, como indica Fernández-Miranda, se ha desperdiciado la oportunidad de regular con más detalle algunas materias controvertidas, sólo esbozadas en el Reglamento, tales como la elaboración de supuestos en los que se puede ejercer el derecho al olvido. Por el contrario, en la Ley se regulan determinados «derechos digitales» que nada tienen que ver con la protección de datos y que requerirían de una ley independiente, como el derecho a la educación digital (art. 80), el derecho a la desconexión digital en el ámbito laboral (art. 88) o los derechos digitales en la negociación colectiva (art. 91).

4. *¿Qué valoración le merecen las aportaciones jurisprudenciales que tanto a nivel nacional como internacional se han hecho a la construcción de este derecho? En concreto, ¿considera suficiente el amparo constitucional del derecho en España ofrecido por el artículo 18.4 de nuestra Carta Magna y el desarrollo que ha realizado el Tribunal Constitucional a partir del mismo?*

LORENZO COTINO HUESO

La jurisprudencia ha sido uno de los focos de reconocimiento y construcción del derecho de protección de datos. Los tribunales han acompañado la normativa europea y nacional que se iba produciendo y han impulsando algunos aspectos o completado lagunas de dicho reconocimiento normativo. Por cuanto al TC español, sigue siendo referencia la STC 292/2000. La misma intentó subrayar las diferencias entre la protección de datos (derivada del artículo 18. 4.º CE) y la intimidad reconocida en el apartado 1.º. Así, se afirmó que es un instituto de garantía de derechos, un derecho fundamental autónomo y que es una dimensión positiva de la intimidad: derecho de controlar el uso de datos en programa informático («habeas data») para impedir un tráfico ilícito, excluir datos de conocimiento ajeno, resguardar la vida de publicidad no querida. Se reconoció un «haz de facultades» y derechos a diferencia del deber de abstención reactivo de la intimidad (art.18.1.º CE).

El 8 de abril de 2014 el TJUE impulsó las necesidades de calidad normativa, declarando contraria al derecho fundamental la Directiva 2006/24/CE de retención de datos de tráfico. A este respecto la muy reciente STJUE de 6 de octubre de 2020 sigue marcando diversas exigencias frente a los rastreos masivos de datos que hacen los Estados por motivos de seguridad. La STJUE de 13 mayo de 2014 del derecho al olvido tuvo un efecto simbólico en cuanto a la extraterritorialidad del derecho de la UE, así como para contener algunos excesos de los buscadores y grandes plataformas. Este nuevo derecho al olvido se ha integrado en España con la STC 58/2018 y la Ley orgánica 3/2018 y ya se va destilando con continua jurisprudencia del TS. Lo cierto es que se trata de un derecho ya casi imposible de deslindar del derecho de rectificación de protección de datos o incluso del derecho de rectificación y de actualización de informaciones en razón de la libertad de información.

Respecto del tratamiento de datos por el sector público, la STC 17/2013 de 31 de enero, aunque dio por buena la ley que permite el acceso por la policía a los datos del registro del padrón municipal, elevó los estándares y garantías. Sin embargo, la realidad del sector público (respecto del que sólo excepcionalmente hay sanciones y su regulación legal muchas veces es poco rigurosa) sigue muy por debajo de lo exigido por dicha sentencia. El TC ha titubeado algo respecto de la posibilidad de utilizar imágenes captadas para otra finalidad (STC 29/2013 frente a la STC 39/2016). En el ámbito del control laboral ha habido ciertas discrepancias entre la jurisprudencia nacional y algunas líneas marcadas por el TEHD, que

también ha oscilado en esta materia (STEDH —Gran Sala— 5.9.2017, Caso Barbulescu II y STEDH 17 de octubre de 2019 de Gran Sala en el caso español de López Ribalda).

En cualquier caso, jurisprudencialmente destaca la STC 76/2019. En primer lugar, porque en menos de cuatro meses se declaró la inconstitucionalidad de una ley. En segundo lugar y por lo que ahora interesa, porque ha sido muy rigurosa respecto de las garantías y la calidad de la ley limitadora del derecho de protección de datos, ya bajo el régimen del RGPD. No obstante, como luego se comentará, la realidad de la legislación española queda muy por debajo del cumplimiento normativo y efectivo de tal nivel de garantías.

El TC español en modo alguno ha sido pionero ni innovador en la protección de derechos frente a la transformación digital. Ha quedado bajo la estela de la legislación nacional y europea, así como de la jurisprudencia supranacional, por lo general más innovadora.

Por cuanto a si es suficiente el actual reconocimiento constitucional, obviamente, sería muy positiva la introducción en el texto constitucional del derecho mismo, así como sus contenidos y elementos estructurales básicos y las diversas garantías ya consagradas, también las autoridades de control. Especialmente sería de interés la proclamación de los principios de la protección de datos y nuevas garantías e incluso nuevos derechos frente a las nuevas amenazas e impactos de la transformación digital en la privacidad, la no discriminación y otros derechos. El texto constitucional —o en su caso una actitud más activista del TC— podría reconocer o destilar derechos frente a los registros en línea, el control laboral, el uso público y privado de la inteligencia artificial y las decisiones automatizadas, podría mencionar el nuevo modelo de responsabilidad proactiva y cumplimiento normativo, exigencia y garantías de seguridad, la necesidad de instrumentos y garantías legislativas frente a los impactos públicos y colectivos de las mismas, así como mencionar el papel de la sociedad civil y, especialmente la necesidad de un papel proactivo de las instituciones y autoridades en la materia. El reconocimiento constitucional de los antedichos contenidos haría que la ya existente regulación legal cobrase un mayor vigor y fuerza normativa.

En cualquier caso y a la espera de un constituyente que nunca parece llegar, también es posible animar a los altos tribunales a volver a hacer una lectura del art.18.4.º CE. De hecho, su texto en modo alguno queda limitado a reconocer el derecho subjetivo de protección de datos y bien puede implicar nuevos derechos, garantías y mandatos constitucionales al legislador para una protección efectiva frente a estas amenazas.

ROSARIO GARCÍA MAHAMUT

Contestando a la primera de las preguntas, sin duda, las aportaciones jurisprudenciales han resultado decisivas e imprescindibles en la construcción del

contenido y garantía del derecho tanto a nivel nacional como internacional y, especialmente, comunitario.

En perspectiva histórica y por lo que afecta a la jurisprudencia nacional, solo basta recordar cómo el reconocimiento del derecho fundamental a la protección de los datos personales como derecho autónomo de contenido propio e independiente del derecho a la intimidad en nuestro ordenamiento partió de las SSTC 290/2000 y la 292/ 2000, de 30 de noviembre. Sentencias que, como tantas veces se ha puesto en valor, consolidaron un camino que comenzó a pergeñarse tras la STC 254/1993.

La LORTAD, la LOPD y sus reformas, así como su Reglamento de desarrollo de 2007, y actualmente la LOPDGDD se han visto complementadas y enriquecidas por una decisiva e incisiva jurisprudencia del Tribunal Constitucional y también del Tribunal Supremo. Todo ello, amén, huelga decirlo, de una valiosísima jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia que han resultado decisivas en la interpretación y aplicación de la normativa interna y/o comunitaria y han coadyuvado a una evolución normativa que, acompasada con una realidad digital que no conoce de fronteras y sí de globalización, no ha conocido parangón como la propia revolución tecnológica.

Ciertamente, la jurisprudencia nacional y comunitaria deben necesariamente contextualizarse en la evolución del propio Derecho de la Unión, que ha generado concretas obligaciones para los Estados miembros. En perspectiva, y a grandes pinceladas solo basta traer a colación, entre otros, el Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981 —completado por el Protocolo adoptado el 18 de mayo de 2018—, el Convenio Europeo de los Derechos Humanos, el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, el art. 16 del Tratado de Funcionamiento de la Unión Europea o el RGPD

Volviendo a las aportaciones de la jurisprudencia interna, no quisiera soslayar que, en contadas ocasiones, ni el Tribunal Supremo (con las limitaciones propias de su competencia) ni el Tribunal Constitucional, a mi juicio, han cumplido con las expectativas. Estoy pensando, por ejemplo, en la STS, Sala Tercera, 4646/2008 o la STC 114/2006. Sin embargo, y en perspectiva, nada ensombrece la decisiva labor desempeñada por ambos en la construcción del derecho. A modo de trazo grueso recordemos de forma más actualizada la enorme trascendencia de la STC 76/2019, que declaró la inconstitucionalidad del primer apartado del art. 58.bis) de la LOREG que incorporó la LOPDGDD a través de su disposición tercera, apartado dos. Tampoco quisiera dejar de mencionar la relevante aportación de la STC 58/2018 que incorpora claramente valor añadido al derecho al olvido complementando el criterio del Tribunal de Justicia sobre la materia.

En la misma línea, cómo obviar, por ejemplo, el paso de gigante que implicó la Sentencia del Tribunal de Justicia (STJUE) de 13 de mayo de 2014, C-131/12 Google Spain, SL y Google Inc *c.* AEPD y Mario Costeja González y el reconocimiento del derecho al olvido digital con claras implicaciones para el derecho interno y su posterior recepción en el RGPD. Y, actualmente, qué decir tiene el

impacto positivo para la defensa del sistema de garantías del derecho a la protección de datos de la reciente STJUE en el asunto C-311/18, *Data Protection Commissioner c. Facebook Ireland and Maximillian Schrems* que ha declarado que la Decisión Escudo de la privacidad es inválida. Al efecto, ha considerado que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas en EEUU no gozaban de una protección equivalente a lo dispuesto en el RGPD. Y, concretamente, que «la primacía de las exigencias relativas a la seguridad nacional, el interés público y el cumplimiento de la ley estadounidense» suponían una clara injerencia en los derechos fundamentales de las personas cuyos datos personales son transferidos a ese país.

En relación con la segunda de las preguntas quisiera recordar una obviedad, pero no por ello carente de importancia, y es que el derecho fundamental reconocido en nuestro art. 18.4 CE es ya un derecho directa y principalmente regulado por una norma europea —básica, aunque no exclusivamente— por el RGPD, independientemente de la competencia del Estado para complementar o desarrollar normativamente algunos aspectos cuando el RGPD así lo establece, ya sea con carácter preceptivo o potestativo. Nada resulta más ilustrativo que el tenor literal del artículo 1, a), segundo párrafo, de la LOPDGD: «El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica». Lo que implica, como también ha subrayado el Consejo de Estado, «un traslado parcial del canon constitucional de protección del derecho fundamental, que, en cuanto se refiere a actividades regidas por el Derecho de la Unión, deberá regirse por la Carta de Derecho Fundamentales de la UE y por la interpretación que realice el Tribunal de Justicia de la Unión».

Dicho lo anterior, a mi juicio, el art. 18.4 CE comienza a romper las costuras de un conjunto de derechos que se expanden e irradian su efectividad sobre derechos que, incluso, demandan ser expresamente reconocidos. A muy corto plazo, los derechos digitales demandarán una categorización constitucional expresa y la protección de los datos personales seguirá constituyendo el nudo gordiano; y, desde luego, no para salvaguardar en exclusiva la intimidad o la privacidad sino como elemento imprescindible para garantizar en su contenido esencial el ejercicio de otros derechos fundamentales y su endógeno sistema de garantías. Cuando pienso en ello, solo me viene la imagen del derecho a la tutela judicial efectiva. En sí mismo es un derecho con contenido propio, pero también es un instrumento fundamental para la defensa de los demás derechos. Algo parecido ocurrirá irremediablemente con el derecho a la protección de datos personales. En sí mismo, obviamente, es un derecho autónomo, pero también será un instrumento decisivo para garantizar el ejercicio efectivo de otros derechos digitales que irremediablemente deberán tener asiento constitucional y legal expreso; con lo que ello conllevará también para el sistema de garantías. Quizás no resulte descabellado crear un orden jurisdiccional específico para resolver los conflictos que se ciernan sobre los derechos digitales en un mundo en red.

PABLO LUCAS MURILLO DE LA CUEVA

Empezaré por la última parte de la pregunta. En España, la aportación del Tribunal Constitucional en su sentencia n.º 292/2000 consistió en dotar de fundamento constitucional a un derecho que ya estaba reconocido y perfilado por el legislador desde 1992 pero al que no había atribuido naturaleza ni denominación. La Ley Orgánica 5/1992, de 29 de octubre, la LORTAD, se limitó a hablar en su exposición de motivos de un nuevo y más consistente derecho a la privacidad de las personas, dando así carta de naturaleza a este anglicismo que, como tantos otros, ha hecho fortuna y se une a la, en apariencia, imparable tendencia a servirse del inglés para nombrar aquello que cuenta con su nombre en perfecto castellano. Pero dejando al margen la colonización del idioma que se está produciendo, sucede que el legislador de 1992 no se atrevió a dar el paso de reconocer como derecho fundamental el de protección de datos a pesar de que el artículo 18.4 de la Constitución le ofrecía, como tiempo después explicó el Tribunal Constitucional, el apoyo suficiente. Más significativo es que tampoco lo hiciera siete años más tarde la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, para acomodar la regulación española a la Directiva 45/96/CE, redujo el alcance del principio de finalidad y abrió espacios a los tratamientos sin consentimiento del afectado aunque introdujera su derecho a oponerse a ellos.

En todo caso, hoy en día, con el reconocimiento efectuado por el artículo 8 de la Carta de los Derechos Fundamentales, el régimen jurídico contenido en el Reglamento (UE) 2016/679 y el fundamento que le prestó el Tribunal Constitucional en el ordenamiento español, me parece suficiente amparo constitucional. No creo que sean precisos ulteriores pasos, fuera ya de la posibilidad de que en una hipotética reforma de la Constitución se incluya entre los derechos fundamentales el de protección de datos. Pero ni esta es una razón para reformarla ni se resentirá el derecho por no estar expresamente mencionado en la Constitución ya que quien puede hacerlo, su intérprete supremo, lo ha encontrado en su seno.

La aportación de nuestro Tribunal Constitucional ha sido, pues, decisiva. Los pronunciamientos que ha hecho después no podían alcanzar la importancia del contenido en la sentencia n.º 292/2000 y se han dedicado a aspectos singulares como, por ejemplo, entre los más recientes, incluir en el llamado derecho al olvido la facultad de prohibir la indexación del nombre y apellidos en los motores de búsqueda internos de los medios de comunicación (sentencia n.º 58/2018).

Por otro lado, el Tribunal de Justicia de la Unión Europea, con sus sentencias en los asuntos Digital Rights Ireland, Google contra España y Schrems, entre otras, ha contribuido, decía, a impulsar los trabajos que llevaron al Reglamento (UE) 2016/679 pues consolidaron la consideración como derecho fundamental del que protege los datos personales. Y en una dimensión más amplia, como es la que le da el Convenio de Roma y sus Protocolos, el Tribunal Europeo de Derechos Humanos ha ayudado a dotarle de contenido sustantivo y tiene ante sí el

reto de interpretar, una vez que entre en vigor, por haber obtenido el número suficiente de ratificaciones, el Protocolo n.º 223, el que pone al día el Convenio n.º 108, de 1981. Será muy importante la labor que realice porque, a diferencia de lo que sucede con el Reglamento (UE) 2016/679, este Protocolo no contempla el derecho a la protección de datos como un límite a la libertad de circulación de datos personales.

MANUEL MEDINA GUERRERO

Atendiendo al claro tenor literal del artículo 18.4 CE, parece evidente que el constituyente «no quiso» consagrar un derecho fundamental autónomo, pues —como se desprende de sus propios términos— este precepto no contiene sino un mandato impositivo de legislación tendente a la garantía de los derechos fundamentales sí reconocidos explícitamente en el texto constitucional. La elevación, pues, de este «mandato impositivo de legislación» a la categoría de específico derecho fundamental es sin duda una relevante «aportación» —la aportación por antonomasia— efectuada por el TC en este ámbito. Licencia jurisprudencial a la que prestó obviamente apoyo la línea seguida los países de nuestro entorno tendente a subrayar la especificidad de la tutela de la privacidad en la esfera de las nuevas tecnologías, llegando en última instancia a su paulatina incorporación como derecho fundamental independiente en los textos constitucionales (desde su pionera incorporación a la Constitución del Land Renania del Norte-Wetsfalia en 1978).

Por lo que hace a la valoración del desarrollo que ha hecho el TC a partir del mismo, creo que ha realizado una atenta y razonable incorporación de las líneas y criterios que han ido fraguando el TEDH y el TJUE. Naturalmente, y pese a la indudable relevancia de la STC 76/2019, aún es pronto para pronunciarse sobre una valoración general del desarrollo jurisprudencial del derecho tal y como ha quedado re-configurado en el nuevo marco normativo. En cualquier caso, en la medida en que el alcance, contenido y límites de este derecho fundamental están esencialmente regulados en el RGPD, parece evidente que el margen de maniobra «creativo» de nuestro TC resulta bastante reducido en el marco del nuevo sistema, deviniendo absolutamente determinantes las pautas que vaya trazando el TJUE al acometer la interpretación del mismo.

ARTEMI RALLO LOMBARTE

La construcción jurisprudencial del derecho a la protección de datos es incuestionable. Un derecho *novísimo*, falto de construcción y tradición dogmática y objeto de una exhaustiva regulación normativa de obtusa comprensión, no hubiese alcanzado el éxito aplicativo que se le reconoce sin la rigurosa y activa

acción jurisprudencial protagonizada por todas las jurisdicciones concernidas. Merecedor de singular reconocimiento resulta el acervo hermenéutico aportado por jurisdicciones altamente especializadas como, en el plano nacional, la Sección 1.ª de la Sala de lo Contencioso Administrativo de la Audiencia nacional, o claramente comprometidas con la salvaguarda de los derechos frente a la tecnología como el TJUE.

El Tribunal de Justicia de la Unión Europea (TJUE) se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global como explicábamos en esta misma Revista poco tiempo atrás («El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet», *Teoría y Realidad Constitucional*, 39, 2017, pp. 583-610).

El impacto mundial de una normativa de protección de datos originariamente europea ha tenido una doble manifestación: la proliferación de regímenes normativos de protección de los datos personales en el resto de los continentes y la obligada adecuación de los servicios tecnológicos globales, independientemente de su origen geográfico, a la normativa europea de protección de este derecho fundamental y, en concreto, a la jurisprudencia de la jurisdicción garante de su efectividad, esto es, del Tribunal de Justicia de la Unión Europea.

La inevitable fuerza expansiva extraterritorial de la jurisprudencia del TJUE resulta especialmente evidente en algunas de sus sentencias —*Caso Digital Rights* (Directiva conservación de datos), *Caso Google* (derecho al olvido) y *Caso Facebook* (Safe Harbour)- que marcan un hito en la evolución de la protección de los datos personales frente a la globalización tecnológica por su impacto mundial, esto es, por la expansión de los estándares europeos de protección de datos al resto de latitudes del planeta. La jurisprudencia del TJUE constituye referencia inexcusable pues ilustra sobradamente los enormes riesgos potenciales para la privacidad del individuo que derivan del uso de servicios y dispositivos tecnológicos en los que se almacena abundante información personal sin que el principio de territorialidad estatal pueda satisfacer las garantías necesarias para evitar la lesión en la intimidad individual.

También el TEDH ha venido configurando un robusto cuerpo doctrinal interpretativo del «respeto a la vida privada» exigido por el art. 8 CEDH del que ha deducido la vigencia de un evolutivo «derecho a la protección de datos personales» que ha adquirido notable trascendencia e impacto jurisprudencial con la revolución tecnológica y la omnipresencia de Internet. Originariamente, los principios generales básicos de esta jurisprudencia sobre protección de datos trajeron causa de actividades de autoridades públicas que, relacionadas con la seguridad pública y la lucha de formas diversas de criminalidad organizada (como el terrorismo), implicaban injerencias en los datos personales y, por lo tanto, en la vida privada: censura; interceptación de correspondencia y de conversaciones de personas detenidas; interceptación de comunicaciones telefónicas en investigaciones criminales y utilización de dispositivos de escucha. De singular interés resulta el análisis de su relevante jurisprudencia sobre almacenamiento y

conservación de información personal por autoridades públicas en el ámbito de la seguridad pública y la justicia penal.

Por el contrario, la relevancia de la jurisprudencia constitucional ha sufrido un significativo retroceso cuantitativo y cualitativo desde que el Tribunal Constitucional atribuyera a la protección de datos rango de derecho fundamental, autónomo del derecho a la intimidad, a partir de la expresa referencia contenida en el art 18.4 de la Constitución. Aunque inicialmente el Alto Tribunal restringió el alcance de este derecho a una mera especificación del derecho a la intimidad, pronto le otorgó la naturaleza de un derecho fundamental autónomo caracterizándolo como un derecho fundamental frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos con un contenido mínimo. Las SSTC 290/2000 y 292/200 marcarían un antes y un después en la jurisprudencia constitucional sobre el derecho de protección de datos. La STC 290/2000 confirmó que el derecho consagrado en el art. 18.4 CE contenía un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos y que, además, constituía, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos. Esta Sentencia supuso un salto cualitativo que se complementaría con la STC 292/2000 reconociendo al derecho de protección de datos un contenido esencial residenciado en el poder de control del individuo sobre el uso y destino de sus datos personales. Con ello, el TC identificaba un instrumento más idóneo ante la eclosión de nuevos peligros procedentes de las nuevas tecnologías que el que podían ofrecer los derechos fundamentales al honor, a la intimidad o a la propia imagen reconocidos en el art. 18 CE.

Sin embargo, tras esta trascendental doctrina constitucional, el TC ha limitado sus pronunciamientos a situaciones concretas con criterios mayoritariamente ortodoxos y coherentes pero, también, con resoluciones harto cuestionables como el ATC 20/2011 (apostasía y libros de bautismo) y las SSTC 76/2019 (olvido) y 58/2018 (art. 58 bis LOREG). La STC 58/2018, de 4 de junio, haciéndose eco de la STJUE de 13 de mayo de 2014 (C-131/12, caso *Google v. Spain*), no ha dudado en proclamar el reconocimiento expreso del derecho al olvido como derecho fundamental con un cuestionable alcance, por desproporcionado, a los motores de búsqueda internos de las websites de medios de comunicación online.

La STC 58/2018 (art. 58 bis LOREG) ofrece algunas peculiaridades de interés. De entrada resulta altamente curioso observar cómo, vistos los dilatados tiempos invertidos en los procesos constitucionales por el TC y el notorio retraso generalizado en sus pronunciamientos, el Tribunal Constitucional resolvió el 22 de mayo de 2019 (en apenas tres meses) un recurso de inconstitucionalidad interpuesto el 5 de marzo de 2019 por el Defensor del Pueblo. Difícil explicar tan extrema diligencia visto el resultado material que comentaremos a continuación.

La STC 76/2019, de 22 de mayo, declaró la nulidad únicamente del primer apartado del art. 58 bis LOREG. Aunque pueda parecer lo contrario, visto un consolidado relato que se aleja bastante de la realidad, la STC 76/2019 validó la constitucionalidad «material» de la casi totalidad del art. 58 bis LOREG y solo, por razones «formales», cuestionó su primer apartado por un solo motivo de técnica jurídico-constitucional: para el TC, la LO 3/2018 no fijaba por sí misma, como le exigiría el art, 53.1 CE, las «garantías adecuadas» para la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Esto es, el TC no cuestionó la constitucionalidad del interés público en la recopilación por los partidos políticos, en el marco de sus actividades electorales, de datos personales relativos a las opiniones políticas de las personas, siempre y cuando se realizara adoptando garantías adecuadas debidamente incorporadas a una ley orgánica como instrumento constitucional idóneo para regular el desarrollo del contenido esencial del derecho fundamental de protección de datos. Lo que hizo el TC fue negar que resultara suficiente la implícita remisión a la potestad normativa de la AEPD ejercida a través de la Circular 1/2019. El Tribunal Constitucional no cuestionó el fondo si no la forma elegida por el legislador para concretar dichas «garantías adecuadas». Si la ley hubiera incorporado sustancialmente las garantías concretadas por la Circular 1/2019 de la AEPD, el TC habría sentenciado la plena constitucionalidad de las previsiones del apartado 1 del art. 58 bis LOREG. Nos hallamos todavía ante la errática comprensión del sistema de garantías constitucionales de los derechos fundamentales aplicado a un derecho fundamental (protección de datos) normativizado plenamente en el ámbito europeo. Tratándose de un derecho fundamental europeo, cuyo contenido esencial y garantías normativas se hallan estrictamente delimitadas por la CDFUE y el RGPD, mantener que los arts. 53.1 y 81.1 CE obligan a incorporar dichas garantías a una ley orgánica implica desconocer la «abducción» operada por el derecho europeo sobre el derecho fundamental a la protección de datos.

LUCRECIO REBOLLO DELGADO

La CE, siguiendo la intencionalidad, que no la literalidad, de la Constitución Portuguesa de 1977, regula la utilización informática. Establece que el reconocimiento de los derechos del art. 18 deben ser considerados como una manifestación concreta del derecho a la integridad moral del art. 15 de la CE. De esta forma tan tangencial, el art. 18.4 de nuestra norma fundamental remite al desarrollo legislativo la limitación del uso de la informática para evitar la colisión directa entre el derecho a la intimidad con las necesidades informáticas, fundamentalmente de los poderes públicos. También tiene implicaciones informáticas el art. 105.b de la CE, el cual posibilita el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, averiguación de los delitos y la intimidad de las personas.

Por una parte, el art. 18.4, se inserta dentro del núcleo dogmático de la Constitución (Sección Primera, del Capítulo Segundo, del Título I), correspondiéndole, por tanto, el mayor grado de protección. Por el contrario, el contenido de mayor virtualidad, en el ámbito de salvaguarda de derechos, es decir el art. 105.b, se sitúa en la parte orgánica de la CE, quedando con ello difuminados sus elementos garantizadores y protectores. Además, su contenido no deja de identificarse con el del art. 20.1.d) CE. Con todo, el reconocimiento constitucional que es leve e inconcreto queda pendiente de una normativa posterior.

En definitiva, no podemos dejar de tener en cuenta las afirmaciones del Tribunal Constitucional, que a nuestro entender resumen de forma acertada la intencionalidad del constituyente, cuando manifiesta al respecto del art. 18.4, que «... de este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales...» (STC 254/93, fundamento jurídico sexto).

No se le podía exigir mucho más a una norma de 1978. Pero esa carencia ha sido suplida tanto por la normativa de la UE, como por la jurisprudencia, con igual atribución de mérito a la nacional y europea. El desarrollo del artículo 18.4 realizado por el TC en sus sentencias 290 y 292 del año 2000 fueron un pilar en el que el ordenamiento jurídico español fundamentó el desarrollo constitucional, y que ha ido contorneando con posterioridad, cumpliendo de forma satisfactoria con su misión constitucional de adecuar las respuestas jurídicas a las necesidades sociales en el ámbito de los derechos y libertades fundamentales. Lo mismo puede afirmarse de la jurisprudencia europea, que tanto desde la labor del TJUE, como del TEDH, han realizado una labor meritoria y eficaz de interpretación y adecuación en el ámbito de la protección de los derechos y libertades fundamentales frente a los retos tecnológicos.

Más recientemente, la Ley Orgánica 3/2018 adapta al ordenamiento jurídico español el RGPD, completa sus disposiciones y garantiza los derechos digitales de la ciudadanía conforme al mandato constitucional establecido en el art. 18.4 (art. 1). La característica más destacable de esta nueva regulación estatal es su remisión constante al RGPD, que se constituye en la norma troncal, siendo aquélla complemento necesario, o en la mayoría de las ocasiones, precisando sus contenidos. A ello se suma la obligación de la normativa estatal de depurar los mandatos jurídicos nacionales que dificulten o imposibiliten la plena aplicación de la normativa europea. Se convierte así la Ley Orgánica 3/2018 en una norma complementaria o de desarrollos concretos del RGPD.

Otro aspecto nuclear de la norma que analizamos viene constituido por los usos de internet, y la transformación digital que se ha producido en nuestra sociedad, y de forma concreta los derechos del ciudadano en internet, a los que se engloba bajo el concepto de derechos digitales (arts. 79 a 97). En esta regulación se aprecia de forma clara la evolución del derecho a la protección de datos de carácter

personal, que requiere de nuevas garantías jurídicas, y que está de forma permanente en evolución, tanto desde la perspectiva de las posibilidades técnicas, como desde las respuestas jurídicas.

Como toda regulación jurídica, tanto el RGPD, como la Ley Orgánica 3/2018, necesitarán de interpretaciones judiciales que aclaren o concreten muchos de sus contenidos, tarea que deberá realizar nuestro Tribunal Constitucional y el Tribunal de Justicia de la Unión Europea, y que será complemento necesario de su vigencia, así como los pertinentes desarrollos reglamentarios, constituyéndose en complemento esencial de la norma.

ANTONIO TRONCOSO REIGADA

La Directiva 95/46/CE, al igual que el Convenio 108 del Consejo de Europa, era técnicamente una buena norma, pero no pudo regular el desarrollo de las tecnologías de la información ni daba respuesta a los conflictos jurídicos que se habían producido en los últimos años. Esto forzó a los Tribunales a resolver sin una norma jurídica previa clara que abordara el conflicto, lo que abocaba a que muchas de sus resoluciones no tuvieran acomodo en un parámetro normativo, sino que fueran un ejemplo de creación del derecho por unos órganos judiciales no especializados, convirtiendo algunas resoluciones judiciales en un caso fortuito. Por ello, se hacía necesario que el legislador europeo y nacional reflexionase sobre los bienes jurídicos en presencia y ofreciera un criterio sobre los derechos que deben prevalecer, teniendo en cuenta el principio de proporcionalidad. Las autoridades de control y los Tribunales disponen ahora del RGPD y de la LOPDGDD que, a diferencia de la Directiva 95/46/CE y de la LOPD, son normas más precisas y de detalle que sirven para dar respuesta a los conflictos jurídicos que se han producido en los últimos años, evitando así las situaciones de desconcierto existentes en el pasado.

Es necesario destacar el importante papel del Tribunal Europeo de Derechos Humanos que incluyó a partir de 1987 dentro del derecho a la vida privada del art. 8 CEDH, el derecho a la protección de datos personales, desgranando en los últimos treinta años una interesante jurisprudencia para el reconocimiento y tutela del derecho fundamental a la protección de datos personales y para la definición de sus elementos principales, en la que ha participado activamente López Guerra. También hay que subrayar la jurisprudencia del Tribunal de Justicia de la Unión Europea acerca del derecho a la protección de datos personales. Muestra de ello es que la primera vez que el Tribunal afirma que «el respeto a los derechos fundamentales forma parte integrante de los principios generales del derecho que el Tribunal de Justicia salvaguarda», salvaguardia que se inspira en «las tradiciones constitucionales comunes a los Estados miembros» es en la Sentencia, de 12 de noviembre de 1969 —caso *Stauder*— que resolvió un litigio de protección de datos personales.

Hay que valorar positivamente las aportaciones jurisprudenciales que han insistido en la importancia de que el respeto a las normas de protección de datos personales esté sujeto al control de una autoridad independiente. Así, el TJUE ha señalado que las autoridades de control son las guardianas de los derechos y libertades fundamentales, subrayando la importancia de la independencia de las autoridades de control nacionales. Para el TJUE, «la mera posibilidad de que las autoridades del Estado puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de estas». Por dos razones: la primera, porque podría dar lugar a una «obediencia anticipada» de las autoridades de control; la segunda, porque dado el papel de guardián de la protección de datos de las autoridades de control, esto exige que las autoridades de control «estén por encima de toda sospecha de parcialidad». En la Sentencia de 8 de abril de 2014 —caso *Comisión/Hungría*—, el TJUE incidió en la importancia de la inamovilidad de sus miembros; en la Sentencia de 16 de octubre de 2012, —caso *Comisión/Austria*—, el TJUE subrayó la autonomía organizativa y de personal y la independencia funcional de la autoridad de control; y en la Sentencia de 9 de marzo de 2010 —caso *Comisión/Alemania*—, también en relación con la autonomía organizativa, el TJUE declaró que la República Federal de Alemania había incumplido las obligaciones de la Directiva «al someter a la tutela del Estado a las autoridades de los Länder». También el TEDH, en la Sentencia de 4 de mayo de 2000 —caso *Rotaru*— consideró que la inexistencia de un procedimiento que asegure los derechos del interesado y controle la actividad de la Administración supone una vulneración de la legislación de protección de datos.

La aplicación del RGPD va a contribuir a suprimir en nuestro país algunas rigideces y exigencias adicionales que no provenían sólo de la legislación de protección de datos sino también de la jurisprudencia del Tribunal Constitucional que incorporó al contenido esencial del derecho fundamental elementos que justamente estaban fuera de la noción generalmente admitida por los juristas de lo que el derecho a la protección de los datos personales significaba. Ese planteamiento tiene que ser valorado teniendo en cuenta que en el plano —evidentemente distinto, en el que no entra el TC— del Derecho europeo, la STJUE, de 24 de noviembre de 2011, condenó a España por una inadecuada transposición de la Directiva 95/46/CE, que no se limitaba a una armonización mínima —no era una Directiva de mínimos— sino que constituía, en principio, una armonización completa que operaba como norma de máximos y que impedía que nuestro legislador nacional introdujera una protección más rigurosa o que estableciera exigencias adicionales. Esta Sentencia afirmó la incorrecta transposición de la Directiva por parte de la legislación española, que no incluyó como supuesto de legitimación del tratamiento la satisfacción de un interés legítimo del responsable —que sí se encontraba en la tradición jurídica de los Estados miembros—, sino que impuso obligaciones adicionales y no estableció la necesaria ponderación con los derechos del interesado en las circunstancias concretas.

El Tribunal Constitucional Federal Alemán ha desempeñado un papel importante en la configuración del derecho a la autodeterminación informativa, teniendo en cuenta que fue su Sentencia sobre la Ley del Censo la que por vez primera proclamó este derecho fundamental. Por ello, es interesante reflexionar sobre las fuentes originales y ofrecer algunas pistas sobre las Sentencias principales del BVerfG, teniendo en cuenta que las Sentencias del TC, TEDH y TJUE, son conocidas entre nosotros y han sido muy bien analizadas por la doctrina. Aunque siempre ha habido y sigue habiendo violaciones individuales de los derechos fundamentales en Alemania, su nivel efectivo de los derechos fundamentales es relativamente alto, incluso en comparación con el resto del mundo, gracias sobre todo al Tribunal Constitucional Federal —Kloepfer—. Este ha dictado una dinámica jurisprudencia que no sólo llenó de contenido los derechos fundamentales existentes sino que también creó nuevos derechos fundamentales. Así, ha señalado que el art. 2.1 GG reconoce un derecho fundamental al libre desarrollo de la personalidad que garantiza cuatro derechos en particular: la libertad general de acción, el derecho general de la personalidad, el derecho a la autodeterminación informativa y el derecho a la confidencialidad e integridad de los sistemas de tecnología de la información. Así, en el contexto del derecho al libre desarrollo de la personalidad, el derecho a la autodeterminación informativa otorga a la persona la facultad —la autoridad— para «decidir por sí misma sobre la divulgación y el uso de los datos personales» —BVerfGE 130, 1; 118, 168; 120, 274—, no sólo en el ámbito del tratamiento automático de datos —BVerfGE 78, 77—, de modo que se evite un «efecto intimidatorio duradero en la percepción de la libertad —BVerfGE 125, 260—. Se protege el «derecho del individuo a decidir en principio cuándo y dentro de qué límites se revelan los hechos personales de la vida» —BVerfGE 103, 21; 80, 367—, incluso si los datos no se refieren a la esfera privada o incluso a la intimidad —BVerfGE 65, 1; Jarass—. Los datos personales están protegidos, también en el ámbito público, independientemente de su sensibilidad —BVerfGE 118, 168; 130, 151—. La utilización de páginas de acceso general en Internet se convierte en una vulneración de un derecho fundamental si los datos se recopilan de manera selectiva y esto da lugar a una situación de peligro particular para el titular del derecho fundamental —BVerfGE 120, 274—. En cambio, no hay injerencia si los datos se separan técnicamente sin dejar rastro y de forma anónima después de su recogida. En el caso de la recopilación de datos de forma anónima con fines estadísticos, no es necesario especificar un propósito concreto —también se permite la recopilación de información «en archivo o en reserva»— pero deben tomarse suficientes precauciones contra la desanonimización y el uso indebido —BVerfGE 65, 1—.

Es especialmente interesante la jurisprudencia del Tribunal Constitucional Federal Alemán en relación con los tratamientos con fines policiales —Hömig—. Así ha señalado que sólo son admisibles las «búsquedas de arrastre» o los rastreos policiales preventivos (comparación electrónica de grandes cantidades de datos de características personales consideradas importantes para la búsqueda) con un

peligro concreto y específico para los intereses jurídicos de alto rango y con causa justificada —BVerfGE 115, 320—. El principio de proporcionalidad exige que las situaciones concretas de peligro o los mayores riesgos de amenazas o violaciones de bienes jurídicos justifiquen el reconocimiento y registro automático de los números de matrícula de los vehículos —BVerfGE 120, 274—. El tratamiento del perfil de ADN —huella genética— de manera preventiva como patrón de identificación restringe el derecho a la protección de datos de una manera constitucionalmente permitida en la medida en que sea indispensable para la protección de los intereses públicos; sólo debería ser posible si, en casos individuales, hay motivos suficientes para suponer que la persona en cuestión volverá a cometer delitos de considerable importancia —BVerfGE 103, 21—. También el Tribunal Constitucional Federal examinó la admisibilidad y límites del uso de medidas de vigilancia secretas, en este caso por la Oficina Federal de Policía Criminal, que son, en principio, compatibles con los derechos fundamentales a fin de evitar los peligros derivados del terrorismo internacional, si bien deben respetar el principio de proporcionalidad —BVerfGE 141, 220, Badura—. En el caso de los ficheros de datos con fines antiterroristas, la conducta íntima de las personas no es suficiente para la inclusión en el fichero. Tampoco es admisible la inclusión general del entorno; en particular, no se permite un registro general de las personas de contacto. En relación con el intercambio de datos entre los servicios de inteligencia y la policía, el BVerfG ha derivado del derecho a la autodeterminación informativa un «principio de separación informativa» —BVerfGE 133, 277— que sólo permite la comunicación en casos excepcionales debido a las diferentes tareas de las autoridades policiales y de los servicios de inteligencia y al importante peso de la intervención —Sachs, Zippelius—. Sigue atrayendo un interés especial en la doctrina alemana si las autoridades pueden comprar datos bancarios luxemburgueses y suizos copiados ilegalmente en un «CD fiscal» por grandes sumas de dinero y utilizar esos datos así obtenidos en procedimientos fiscales penales. Toda utilización de información obtenida ilegalmente constituye una nueva violación de los derechos fundamentales y está sujeta al criterio de proporcionalidad, también en los procedimientos penales —BVerfGE 130, 1—. Se requieren razones convincentes y de peso —BVerfGE 80, 367—. Esto se aplica, en particular, a los datos obtenidos en forma secreta —BVerfGE 117, 202—. Inicialmente parece que la jurisprudencia señala que una prohibición general de explotación sólo debe aplicarse en caso de violaciones procesales graves, deliberadas o arbitrarias en las que se hayan desatendido de manera sistemática las salvaguardias de los derechos fundamentales, pero que en cada caso concreto debe establecerse un equilibrio entre el interés de la persecución penal y la protección de la esfera personal —véase el cuestionamiento que hace Hufen—.

En especial hay que señalar que el Tribunal Constitucional Federal Alemán en la Sentencia de 27 de febrero de 2008 —sobre búsquedas en línea— ha señalado otro derecho dentro de los derechos generales de la personalidad, que es el derecho fundamental a garantizar la confidencialidad e integridad de los sistemas

de tecnologías de la información —BverfGE 120, 274—. El trasfondo que dio lugar a alumbrar este nuevo derecho fundamental fue el intento del Estado de Renania del Norte-Westfalia de permitir que órganos estatales realizaran una infiltración secreta en un sistema de tecnología de la información que permitiera la supervisión de su uso y la lectura de sus medios de almacenamiento, mediante la instalación inadvertida de un software de vigilancia en la computadora, que enviaba la información a las autoridades a través de Internet. El alcance de la protección del nuevo derecho fundamental comprende los siguientes elementos —Epping—: debe ser un sistema de tecnología de la información (ordenador personal, dispositivos de navegación, teléfono, dispositivos electrónicos en el hogar o en los vehículos de motor, etc.); que es utilizado por el interesado como propio y al que sólo tienen acceso las demás personas autorizadas, lo que incluye también la información que se almacena en servidores externos con carácter confidencial —BVerfGE 141, 220—; y que contiene una cantidad sustancial de datos personales que permiten sacar conclusiones sobre las características y el comportamiento del usuario. El Tribunal estableció que las restricciones a este derecho fundamental deben cumplir en particular con el principio de proporcionalidad. De esta forma, una infiltración secreta en un sistema de tecnología de la información sólo es admisible si existe un indicio real de un peligro concreto para un bien jurídico sumamente importante —la vida, la integridad física, la libertad de la persona o los intereses generales del público en general, cuya amenaza ponga en peligro los fundamentos o la existencia del Estado o los fundamentos de la existencia humana—. Además, tal medida requiere una orden judicial porque al igual que ocurre con las escuchas en las viviendas, esta también es un área central de la vida privada que está fuera del control del Estado, siendo la prohibición de exceso una barrera particular. El Tribunal diferenció esta nueva expresión del derecho general de la personalidad —la protección de los sistemas de tecnología de la información, en particular los ordenadores—, del secreto de las telecomunicaciones —art. 10 GG— y de la inviolabilidad del domicilio —art. 13 GG—, así como del derecho a la autodeterminación informativa, de manera que sólo es aplicable en la medida en que no sean pertinentes los otros derechos fundamentales especiales —BVerfGE 124, 43—. La especificación de este nuevo derecho informático básico —Mannsen— tiene en cuenta la «importancia de la utilización de los sistemas de tecnología de la información para el desarrollo de la personalidad» —BVerfGE 141, 220—. En este sentido, es una invasión de mayor peso que muchas otras invasiones al derecho general de la personalidad —BVerfGE 120, 274—. Si el derecho a la autodeterminación informativa ofrece una protección especial contra la reunión de datos individuales por terceros, el derecho a la confidencialidad e integridad de los sistemas de tecnología de la información garantiza la protección contra la posibilidad de infiltración, espionaje y manipulación de nuestros sistemas como resultado de su conexión en red —Katz—, porque se utilizan en todas partes, tienen un significado similar al del espacio vital personal y requieren medidas de protección similares —Kingreen—. El Tribunal

Constitucional Federal sólo ha abordado el derecho básico a la confidencialidad y la integridad de los sistemas de tecnología de la información como un derecho de defensa contra los ataques del Estado. No obstante, es necesario concretar los efectos de este derecho fundamental entre los particulares.

CAMINO VIDAL FUEYO

La valoración de la jurisprudencia, tanto nacional como internacional, es muy positiva. Si a la dificultad que implica regular pormenorizadamente todas las posibles injerencias de las nuevas tecnologías en los derechos fundamentales, le unimos la lentitud del legislador frente al acelerado avance tecnológico, nos encontramos ante un escenario en el que jueces y tribunales se convierten en garantes imprescindibles de este derecho.

El papel del Tribunal Constitucional español ha sido determinante. Como es sabido, la Constitución española no recoge el derecho a la protección de datos de manera explícita, por lo que ha sido la jurisprudencia constitucional la que ha construido un derecho fundamental *ex novo* a partir del art. 18.4 CE que, en puridad, se limita a hacer un llamamiento al legislador para que limite el uso de la informática en defensa del derecho al honor y a la intimidad personal y familiar de las personas. Ya en la temprana STC 254/1993 (en la que el Tribunal concede el amparo a un ciudadano al que la Administración del Estado le negaba la información solicitada respecto de los datos de carácter personal existentes en ficheros automatizados de naturaleza pública), así como en la STC 202/1999 (en la que se fija jurisprudencia indicando que el almacenamiento en soporte informático de los diagnósticos médicos del trabajador, sin mediar su consentimiento expreso, carece de apoyo legal y supone una restricción desproporcionada del derecho fundamental a la intimidad y a la libertad informática), el Tribunal Constitucional va configurando el contenido del derecho a la protección de datos, indicando que del art. 18.4 CE se desprende un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos, que es, además, en sí mismo: «un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos» (STC 254/1993, FJ 6, doctrina que se reitera en las SSTC 143/1994, FJ 7; 11/1998, FJ 4; 94/1998, FJ 6, y 202/1999, FJ 2). Esta doctrina se consolida definitivamente en la STC 292/2000, en la que ya se reconoce de forma clara un derecho fundamental autónomo: el *habeas data* (FJ 5).

A partir de estas sentencias y a lo largo de los últimos veinte años, creo que el TC ha venido elaborando una sólida jurisprudencia a través de la que se ha dotado de contenido al derecho fundamental a la protección de datos de carácter personal, partiendo de la consideración de que, si bien el derecho a la intimidad permite garantizar una esfera reservada de la persona, el derecho a la protección

de datos atribuye un poder de disposición y control sobre la información personal, incluso cuando sea accesible a terceros.

Excedería el objeto y finalidad de esta breve encuesta exponer con detalle las principales sentencias dictadas por el TC en los últimos años, pero creo que es de cita obligada la reciente STC 58/2018, en la que se configura el contenido constitucionalmente protegido de un derecho no reconocido hasta el momento, el «derecho al olvido digital» como proyección del derecho al honor, a la intimidad (art. 18.1 CE) y a la protección de datos de carácter personal (art. 18.4 CE), sentencia que se dicta en relación con las hemerotecas digitales, al ser consideradas uno de los ámbitos a través de los que se puede manifestar el ejercicio de las libertades informativas. En este sentido, el TC configura el derecho al olvido como el derecho a la supresión de los datos personales recogidos en las hemerotecas digitales cuando ya no son necesarios en relación con los fines para los que fueron tratados.

En el espacio europeo, tanto el Tribunal Europeo de derechos Humanos (TEDH) como el Tribunal de Justicia de la Unión Europea (TJUE), vienen dictando una importante jurisprudencia que viene a reforzar la protección de los datos personales que se deriva del Convenio Europeo de Derechos Humanos y de de la Carta de los Derechos Fundamentales de la Unión Europea. Así, en la Sentencia del TJUE de 13 de mayo de 2014, en el caso Google Spain vs Agencia Española de Protección de Datos, se dejó claro que el Derecho europeo y, más concretamente, la legislación española, son aplicables a Google, toda vez que la empresa cuenta con un establecimiento en territorio europeo. De otra parte, la Sentencia consideró que las operaciones técnicas que realizan los motores de búsqueda para encontrar la información en Internet se integran en la definición de «tratamiento» que ofrece la Directiva europea, y que los propios motores de búsqueda son los responsables de ese tratamiento porque deciden sobre los medios y sobre sus fines. Para la Sentencia, la difusión y accesibilidad universales que ofrecen los motores de búsqueda pueden lesionar derechos de las personas de una forma mucho más intensa y grave que la publicación original de la información. El Tribunal señala expresamente que no es necesario que se cause un perjuicio para ejercer el derecho frente al buscador.

Asimismo, en la importante Sentencia Schrems I, de 6 de octubre de 2015, el TJUE resuelve la reclamación de una persona física cuyos datos personales fueron transferidos desde la Unión Europea a Estados Unidos a través de *Facebook Ireland*. El Tribunal dicta un fallo en el que invalida la Decisión 2000/520 de la Comisión Europea sobre el Acuerdo de Puerto Seguro, que regulaba la transferencia de datos personales desde la Unión Europea a Estados Unidos, por no cumplir con las garantías relativas a la protección de datos personales derivadas de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea y en 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.

Más recientemente, en la Sentencia Schrems II, de 16 de julio de 2020, el Tribunal de Justicia, a la luz de la Carta y del nuevo Reglamento (UE) 2016/679, se ve en la necesidad de declarar contraria al Derecho de la Unión la decisión 2016/1250 de la Comisión Europea relativa al llamado «Privacy Shield». Una de las razones por las que el TJUE consideró el «Escudo de Privacidad» contrario a Derecho es la imposibilidad de que los interesados europeos puedan defenderse ante los tribunales de Estados Unidos en caso de que accedan a sus datos personales.

A partir de esta jurisprudencia, lo importante es que el nivel de protección de un ciudadano europeo en terceros países a los que se trasfieran sus datos tiene que ser equivalente al nivel de protección existente en la Unión Europea. Así, una normativa ratificada por la Unión Europea que no prevea la posibilidad de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen, o para obtener su rectificación o supresión, no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta.

5. *La intervención del legislador en materia de protección de datos resulta imprescindible. ¿Cómo valora la regulación realizada tanto a nivel nacional como comunitario? Y en concreto ¿qué opina de su extensión, complejidad y accesibilidad para los ciudadanos? ¿Y desde el punto de vista de la justificación y previsión de límites al derecho?*

LORENZO COTINO HUESO

En España hubo una Ley Orgánica 5/1992 de protección de datos incluso antes del reconocimiento de la protección de datos como derecho fundamental por el TC, algo que no ha sucedido por ejemplo con el derecho de acceso a la información pública. Luego, la Ley orgánica 15/1999 transpuso la Directiva de 1995 y supuso un nuevo impulso. Lo mismo sucedió con su reglamento de desarrollo (Real Decreto 1720/2007). Estas regulaciones generales globalmente han sido adecuadas y han permitido crear un fuerte acervo normativo, jurisprudencial y de resoluciones de las autoridades independientes. Puede incluso afirmarse que se ha pretendido situar al estándar español de protección entre los más altos de la UE, intentando igualarse a países como Alemania. Sin embargo, la realidad es que se ha conformado durante mucho tiempo un modelo formalista y bastante burocratizado en el que primaba un mínimo cumplimiento normativo para evitar sanciones, pero no para aportar verdaderas garantías a la protección de datos. Al mismo tiempo, este modelo normativo y la acción del regulador (especialmente la AEPD) no ha tenido la suficiente flexibilidad ni visión para facilitar la innovación y el desarrollo tanto en el sector privado como en el sector público. La protección de datos ha sido una excusa y una amenaza constante lastrando posiblemente un mejor desarrollo de tecnologías e industrias relacionadas con la nube,

los grandes datos y la llamada revolución 4.0. Diversos países de la UE han demostrado que esta innovación sí que era posible con un suficiente respeto por la privacidad y la protección de datos. No obstante, en la Ley orgánica 3/2018 resulta especialmente positiva la regulación de la investigación biomédica. Por el contrario, el injerto de la regulación de los «derechos digitales» introducido sin reposo en el último momento ha sido particularmente desacertado. Por lo general, implica una regulación vacía sin contenido normativo o, en el caso del control laboral, claramente insuficiente y que genera gran inseguridad jurídica. A fines de 2020 parece que se quiere enmendar con una *carta de derechos digitales*, de dudoso alcance.

El RGPD ha incorporado el nuevo modelo de responsabilidad proactiva para garantizar el cumplimiento normativo de manera preventiva. Este modelo de corte anglosajón parece mucho más útil que el modelo burocratizado español meramente reactivo. El RGPD mantiene el consentimiento y los derechos y garantías de la protección de datos, incluso con nuevos derechos, asimismo refuerza positivamente la obligación de transparencia e información al afectado. En todo caso, hay que apostar mucho más por el cumplimiento de los principios (art. 5) y las normas objetivas de protección de datos y la vigilancia de las autoridades. Asimismo, no hay que perder de vista que es nulo el consentimiento del interesado para tratar datos desproporcionados e innecesarios (art. 7.4 .º RGPD). Y hoy día este fenómeno es casi la regla general de muchos tratamientos por parte de plataformas y grandes tecnológicas. La llamada seudonimización va a pasar ser la medida tecnológica estrella para garantizar los derechos subjetivos de los afectados, dado que quienes manejan los datos personales no tienen acceso a la identidad de sus titulares. No obstante, pese a que no se manejen datos identificables y en la línea de lo expuesto, no hay que perder de vista el impacto social y colectivo de los tratamientos de datos anonimizados o seudonimizados.

En todo caso es necesario avanzar respecto de la protección de la privacidad, protección de datos y otros derechos que quedan especialmente afectados por los grandes datos, el Internet de las cosas, los algoritmos y la inteligencia artificial. Y precisamente el enfoque regulatorio futuro va a seguir los pasos del modelo proactivo y preventivo del RGPD. Asimismo, las garantías frente a los perfilados y decisiones automatizadas (artículo 22 RGDP) sin duda van a ir extendiéndose en los próximos años por la vía jurisprudencial o normativa. El camino regulatorio parece adecuado sin perjuicio del tiempo y dificultades que va a necesitar el reajuste del modelo, así como las adaptaciones que se requieren por la transformación digital. Como se ha afirmado anteriormente, sigue siendo necesario un enfoque regulatorio centrado en el impacto colectivo en los derechos y en los bienes constitucionales, pero no tan centrado en los derechos individuales.

Debe decirse que, de cara a la ciudadanía, el texto normativo del RGPD es casi incomprensible incluso para los especialistas, mientras que sus más de cien considerandos son bastante accesibles, aunque no siempre se corresponden con el texto normativo. Las dificultades se agravan por la necesidad de manejar como

referentes el RGPD a la vez de la ley orgánica española. De hecho, el antiguo reglamento de desarrollo sigue vigente.

A esta regulación general del RGPD y la ley orgánica la acompañan incontables leyes que imponen límites específicos al contenido del derecho (excepciones al consentimiento, al deber de información, a los derechos concretos…). Como se ha expuesto, la jurisprudencia constitucional ha mantenido un alto nivel de exigencias y garantías constitucionales de la legislación y su calidad. Sin embargo, contrasta con la realidad del ordenamiento jurídico y de su aplicación. Lo cierto es que muy buena parte de las limitaciones que se recogen en numerosas leyes españolas no cumplen ni los altos estándares del TC ni, sobre todo, las fuertes exigencias para los límites al derecho que establece el artículo 23 RGPD (justificación, garantías específicas, etc.).

ROSARIO GARCÍA MAHAMUT

En relación con la primera de las cuestiones, y en perspectiva histórica, debo poner en valor la labor de nuestro legislador. A mi juicio, en términos globales, ha estado a la altura de las circunstancias propias de su tiempo. Ningún legislador es perfecto; sin embargo, el legislador español ha vuelto a incorporar novedades allanando el camino de nuevos derechos que, aunque fueran incluso de carácter programático, requerían ser perfilados y contextualizados jurídicamente. Esto es justamente lo que ha ocurrido con la LOPDGDD y el decálogo de derechos digitales. En el contexto normativo comunitario, el RGPD constituye un avance sin parangón, independientemente de que determinadas apuestas, tanto desde una perspectiva formal como material, sean susceptibles de mejora y objeto de reformas futuras. En esta línea veremos qué resultado arroja la concreción de las distintas cláusulas abiertas en cada uno de los ordenamientos nacionales. Sin embargo, y paralelamente al avance que propicia la aplicación del RGPD, —con sus incertidumbres y complejidad— se observa una hipernormatividad comunitaria con una variedad de Reglamentos que, afectando al tratamiento de datos personales, no coadyuva a sistematizar en los distintos ordenamientos nacionales y ámbitos afectados aspectos claves del ejercicio, límites y garantías de los derechos afectados. Ello, a mi juicio, resta seguridad jurídica y a la postre irá en detrimento del efecto homogeneizador del RGPD.

En cuanto a la extensión y complejidad y accesibilidad para los ciudadanos de la normativa de protección de datos (LOPDGDD y RGPD) debo afirmar con rotundidad que la complejidad e inaccesibilidad son totales y absolutas. He defendido y argumentado en diversas ocasiones que el resultado de la técnica legislativa por la que optó nuestro legislador escapa de la comprensión de los ciudadanos e, incluso, de los operadores jurídicos. Difícilmente se puede comprender el alcance de los mandatos contenidos en la Ley que desarrolla un derecho fundamental sin tener el RGPD delante. Esto plantea serias dudas desde la perspectiva

de la seguridad jurídica. La remisión de la Ley al RGPD es constante. Y no cabe soslayar que, como se recuerda en la propia memoria de análisis de impacto normativo del anteproyecto de LOPD, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos. Y, en su vertiente negativa, implica la obligación para los Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo.

La estrategia legislativa, a mi juicio, ha resultado en gran medida disfuncional porque la LOPDGDD posee una naturaleza sui generis y no es una norma de transposición sino de integración sistemática del ordenamiento de la Unión que persigue el objetivo de adaptarse a las nuevas necesidades y exigencias de la UE, fomentando una mejor comprensión práctica de las exigencias del RGPD por parte de los ciudadanos, pero dudo mucho que tal objetivo se consiga. Ello, independientemente de que nuestra ley de protección de datos incluya todo un título dedicado al desarrollo de los derechos digitales.

Por otro lado, no podemos obviar el conjunto de disposiciones dispersas que afectan a distintos aspectos de la protección de datos y que podían haber sido implementadas y sistematizadas en nuestra LOPDGDD. Es cierto que la insatisfacción derivada del contenido y de la técnica, que genera tanto la naturaleza del RGPD como su propia complejidad, desde el punto de vista de la técnica legislativa interna, es un sentimiento compartido por especialistas en sus respectivos ordenamientos. Como cierto es que han utilizado diversas técnicas legislativas, unos Estados han optado por aprobar nuevas normas de protección de datos (Alemania y España) y otros por modificar su legislación (Austria o Francia). Del mismo modo que algunos de los ordenamientos han implementado la Directiva 2016/680 y otros —como España—, no.

PABLO LUCAS MURILLO DE LA CUEVA

Ya me he referido al planteamiento que ha llevado al Reglamento (UE) 2016/679. Dejando ahora al margen la relación que establece entre el derecho a la protección de datos y la libertad de su circulación, es evidente que cambia notablemente los presupuestos sobre los que descansaba el régimen jurídico precedente. Si nos situamos en la perspectiva del observador español, podremos comprobarlo sin dificultad. La LORTAD y la LOPD distinguían entre ficheros de titularidad pública y ficheros de titularidad privada y articulaban a partir de esa distinción sus respectivas regulaciones, las cuales apuntaban, principalmente, a la actuación de la Agencia Española de Protección de Datos frente a los incumplimientos de la Ley Orgánica. Aunque la Directiva 95/46/CE se centró en el plano dinámico de los tratamientos en vez de en el estático de los ficheros, la LOPD,

elaborada según se dijo en su día, para adaptar el régimen previsto en la LORTAD a las exigencias de aquella, no modificó el esquema anterior.

El Reglamento (UE) 2016/679, un texto denso y difícil que ocupa 88 páginas del Diario Oficial de la Unión Europea, treinta y una de ellas de considerandos, prescinde de esa distinción y del concepto de fichero y, sin olvidar las actuaciones *a posteriori*, en especial las punitivas, que endurece notablemente, opta con claridad por soluciones preventivas dirigidas a asegurar que los tratamientos de datos sean respetuosos con los principios materiales y con los derechos de los afectados que reconoce y fortalece, empezando por el de consentir los tratamientos en los casos en que es necesario. A ese fin responde la importancia que da a los responsables y a los encargados de los tratamientos y a la seguridad de los datos. También, la previsión de la evaluación de impacto y de la consulta previa así como la figura, especialmente relevante, del delegado de protección de datos. Los códigos de conducta y los mecanismos de certificación y los sellos y marcas de protección de datos completan los instrumentos encaminados al objetivo de anticiparse y evitar las posibles infracciones. Potencia, además, a las autoridades de protección de datos cuya cooperación requiere y organiza y crea un Comité Europeo de Protección de Datos que preside el edificio institucional específico, encargándole dirimir conflictos, orientar y asesorar, así como trazar directrices.

A su vez, la Ley Orgánica 3/2018, de 5 de diciembre, es un texto de máximos. Quiero decir que, ante la alternativa de limitarse al complemento imprescindible del Reglamento o aprovechar la ocasión para incluir contenidos adicionales, nuestro legislador optó francamente por esta segunda vía. Así ha resultado un texto legal mucho más extenso y complicado que la LOPD y lleva, además, el añadido de los derechos digitales de la ciudadanía, según los denomina, en su mayor parte ya previstos en el Reglamento o meramente programáticos y alguna previsión que ha sido declarada inconstitucional (sentencia del Tribunal Constitucional 76/2019).

El material normativo que ofrecen el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 es, en conjunto, de difícil comprensión para quien no esté familiarizado con el derecho a la protección de datos y previsiblemente dará lugar a numerosas controversias. El estilo del primero es el habitual en las disposiciones emanadas por la Unión Europea: eminentemente técnico y especializado. Al ciudadano no le ayudará a conocer cómo defender los derechos que le reconoce. Los propios autores del Reglamento fueron conscientes, no sólo del cambio que éste supone respecto a la legislación precedente en la materia, y de la necesidad de adaptación de las legislaciones nacionales sino, también, de las dificultades que implica su aplicación. De ahí que previeran una *vacatio legis* de dos años, que, como es sabido, en nuestro caso no fue suficiente para que se aprobara a tiempo una nueva Ley Orgánica por las circunstancias derivadas de los resultados electorales habidos a partir de 2015.

Por lo que se refiere a la nueva orientación, no creo que sea una mala idea apostar por anticiparse a los problemas mediante instrumentos que impidan su

aparición o permitan atajarlos antes de que causen perjuicios. Ahora bien, el modelo elegido necesita de numerosos profesionales bien preparados para que funcione. Es verdad que en los últimos años han aumentado significativamente los despachos y entidades dedicados a los problemas surgidos con motivo del tratamiento de datos personales y que hay múltiples iniciativas dirigidas a impartir formación en la materia. No sé, sin embargo, si son suficientes para nutrir las necesidades de las empresas y de las Administraciones Públicas. Y tampoco sé si la Agencia Española de Protección de Datos cuenta con los medios precisos para hacer frente a la enorme labor que tiene ante sí.

MANUEL MEDINA GUERRERO

Desde la aprobación del RGPD, el derecho que nos ocupa presenta la particularidad de tratarse de un derecho fundamental que en lo esencial está regulado directamente por el legislador europeo, pasando las Cortes Generales a desempeñar al respecto una función secundaria. La vigente Ley Orgánica 3/2018 se limita, pues, a desarrollar o complementar lo previsto en el RGPD.

Dicho esto, no puede soslayarse que el RGPD tiene la singularidad de contar con más de setenta «cláusulas de apertura», que atribuyen a los Estados miembros un cierto margen de maniobra normativa para regular determinadas materias. Esta flexibilidad se proyecta a aspectos muy relevantes, como la configuración de algunas bases de tratamiento especialmente aplicables al sector público [artículo 6. 1 c) y e) en conexión con artículo 6.2 y 6.3] o la fijación de restricciones a los tratamientos de categorías especiales de datos [así sucede con seis de las diez circunstancias enumeradas en el artículo 9.2 RGPD: las letras a), b), g), h), i) y j); así como con la habilitación contenida en el art. 9.4 para introducir condiciones adicionales respecto al tratamiento de datos genéticos, biométricos y datos relativos a la salud].

Quizá una especial mención merezca el artículo 85 RGPD, cuyo apartado primero dispone que los *«Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información...»*. Se trata, pues, de un deber para los Estados, pero lógicamente, al tiempo, es también una habilitación a los legisladores nacionales: les confiere un generoso margen de libertad de configuración en orden a determinar cómo y en qué medida resultan de aplicación a la prensa las disposiciones del RGPD. En virtud del propio RGPD, los legisladores nacionales pueden (y deben) establecer en la esfera periodística normas específicas que sustraigan a la misma del régimen general fijado por el RGPD. Por lo demás, el ámbito material al que puede proyectarse esa libertad de conformación normativa es bastante amplio, pues, siguiendo de cerca el precedente del artículo 9 de la Directiva, según dispone el artículo 85.2 del Reglamento, prácticamente toda la arquitectura institucional del RGPD resulta asequible para el legislador nacional, salvando los

considerados materialmente intangibles Capítulos I («Disposiciones Generales») y VIII («Recursos, responsabilidad y sanciones»), a los que se suman por razones obvias los Capitulos X («Actos delegados y actos de ejecución») y XI («Disposiciones finales»). Por tanto, puede el legislador nacional operar en el propio ámbito funcional de las autoridades independientes de control cuando se trata de resolver las frecuentes colisiones entre el derecho a la libertad de información y el derecho a la protección de los datos personales. Pero, como ya sucediera con la anterior LO 15/1999, la vigente LO 3/2018 omite toda referencia a la conciliación entre ambos derechos fundamentales.

En cualquier caso, importa recordar que el RGPD no agota la regulación del derecho que nos ocupa, ya que el tratamiento de datos personales por las autoridades competentes para fines de prevención, investigación, detención o enjuiciamiento de infracciones penales o de ejecución de sanciones penales queda fuera de su ámbito de aplicación [art. 2.2 a)]. La regulación de este sector material se efectúa en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, cuya fecha máxima de transposición era el 6 de mayo de 2018. Sin embargo, a diferencia de otros países, como Gran Bretaña o Alemania, que optaron por aprobar una sola ley que venía, por una parte, a acomodar su normativa interna al RGPD y, por otro lado, a transponer la referida directiva, nuestra LO 3/2018 no aborda esta segunda tarea, que aún se halla pendiente cuando se escriben estas líneas. Estos tratamientos, pues, se siguen rigiendo por la derogada LO 15/1999, de conformidad con lo dispuesto por la Disposición transitoria cuarta de la LO 3/2018.

Por lo que atañe a la complejidad de la normativa reguladora del derecho y a su accesibilidad para la ciudadanía, ya hicimos mención arriba al hecho de que el enfoque «proactivo» sobre el que se estructura el RGPD suma una dificultad adicional a una materia ya de por sí compleja. A lo que habría que añadir la circunstancia de que el RGPD procure descender con cierto detalle a regular aspectos concretos, a fin de evitar que se produzca una excesiva dispersión normativa en el desarrollo del mismo por los Estados miembros. Ciertamente, el marco normativo no resulta de fácil comprensión para los titulares del derecho. De ahí, probablemente, el énfasis que haya puesto el RGPD en asegurar la transparencia de la información por parte del responsable de tratamiento (arts. 12 a 14), imponiéndole que se facilite la misma al interesado «*en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*», en particular cuando la información se dirija *«específicamente a un niño»* (art. 12.1).

ARTEMI RALLO LOMBARTE

Mas bien al contrario, *a priori* pudiera parecer que la intervención del legislador nacional, vista la opción normadora del legislador europeo (RGPD), resultaba perfectamente prescindible e, incluso, improcedente. Por ello, llama extraordinaria

la atención la propia existencia y extensión de la legislación nacional (LOPDGDD) pero no tanto su complejidad y difícil accesibilidad (notas que comparte con el RGPD) por tratarse de elementos desgraciadamente característicos de toda normativa de protección de datos.

El RGPD goza de alcance general, es directamente aplicable en todos los Estados miembros y resulta obligatorio en todos sus elementos pero una amplia jurisprudencia del TJUE permite acotar el alcance de la capacidad legislativa de los Estados miembro sobre las materias reguladas por el RGPD como hemos desarrollado en «El nuevo derecho de protección de datos» (*Revista Española de Derecho Constitucional*, 116, 2019, pp. 47-74).

El RGPD desplazó la normativa interna de protección de datos convirtiéndose en la norma primaria de protección de datos, de directa aplicación en todo el territorio nacional, sin necesidad de norma alguna de transposición. Pero esta derogación implícita no basta, ya que el principio de seguridad jurídica obliga a una depuración del ordenamiento español de protección de datos iniciada con la derogación explícita realizada por la LOPDGDD de todas las normas nacionales que resulten incompatibles con el RGPD. Además, el RGPD hizo uso profuso de la posibilidad reconocida por la jurisprudencia europea para habilitar a los Estados miembros a *completar* su regulación. El RGPD contiene una infinidad de remisiones al Derecho de los Estados miembros posibilitándoles su adaptación al ámbito nacional hasta el extremo de debilitar extraordinariamente su potencia armonizadora y convertiéndose en un *tertium genus* en el sistema de fuentes del derecho europeo con cuerpo de Reglamento pero alma de Directiva. Los ejemplos de esta índole son muy variados: posibilidad de que los Estados excepcionen determinadas categorías de datos de las reglas generales del RGPD, expresa obligación de los Estados para desarrollar el RGPD, etc. La LOPDGDD ofrece múltiples supuestos de habilitación expresa del RGPD al legislador para regular supuestos específicos como la fijación en 14 años de la edad de consentimiento de los menores; la determinación de la ley como norma habilitada para regular los tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos; las categorías especiales de datos; los datos de naturaleza penal; o la conformación de las Autoridades de protección de datos (AEPD y Autoridades autonómicas).

Aún así, las habilitaciones expresas contenidas en el RGPD no agotan las posibilidades normativas del legislador español por cuanto la jurisprudencia europea admite, a modo de habilitaciones implícitas, que la adaptación nacional del RGPD puede atender a reglas genéricas a fin de adaptar el RGPD a las tradiciones jurídicas propias y al contexto nacional y garantizar eficazmente la aplicación del RGPD. La numerosas habilitaciones expresas del RGPD y estas genéricas finalidades perseguidas por la LOPDGDD han amparado un desarrollo profuso del RGPD que afecta a su vocación de obligatoriedad y aplicabilidad directa al desdibujar su propia existencia ante sus destinatarios nacionales. Ahora bien, la jurisprudencia europea obliga a que la adaptación nacional preserve la visibilidad

del RGPD y la trascendencia jurídica de su existencia evitando una apariencia de norma interpuesta que debilite su alcance jurídico. Y, sin lugar a dudas, la LOPDGDD ha cumplido esta exigencia con creces en sus 251 referencias al RGPD.

La adaptación del RGPD a las *tradiciones jurídicas propias* tiene múltiples manifestacions en la LOPDGDD como la ejemplificación de tratamientos excluidos del RGPD por no estar en el ámbito de aplicación del Derecho de la Unión (régimen electoral general, Registros Civil, de la Propiedad y Mercantiles), la regulación de los datos de personas fallecidas, la regulación específica de tratamientos concretos (datos de contacto, empresarios individuales y de profesiones liberales, información creditícia, operaciones mercantiles, vigilancia, exclusión publicitaria o denuncias internas). La jurisprudencia europea no permite la reproducción literal de previsiones del RGPD para evitar la apariencia de una supuesta transposición por el legislador nacional que debilite su fuerza aplicativa uniformadora al provocar confusión al justiciable en torno a la norma alegable y los diferentes elementos constitutivos que les resulten predicables. Algunos supuestos de reproducción literal o remisión al RGPD de la LOPDGDD pueden llevar a confusión por parecer impertinentes cuando, en realidad, resultan necesarios para garantizar la complitud del sistema español de protección de datos. En definitiva, el RGPD admite que la LOPDGDD lo adapte y complete siempre que no ponga en cuestión sus objetivos ni obstaculice la armonización jurídica que persigue. La norma nacional debe procurar seguridad jurídica y eficacia del RGPD pero nunca implicar una normación exhaustiva que excluya o restringa las potencialidades aplicativas del RGPD.

Este nuevo Derecho de protección de datos constituye un ejemplo paradigmático de la sustancial alteración de nuestro sistema de fuentes del Derecho. La primacía del Derecho de la Unión sobre el Derecho interno tiene una principal manifestación, como ya hemos visto, en la abducción del derecho constitucional consagrado en el art. 18.4 CE por los arts. 8 CDFUE y 16 TFUE, por los instrumentos jurídicos que los desarrollan (RGPD) y por el canon hermenéutico impuesto por la jurisprudencia europea. Sin embargo, una manifestación aún más incisiva en la alteración de las fuentes del Derecho español la encontramos en la desnaturalización de la ley orgánica como norma supuestamente llamada a desarrollar el derecho fundamental de protección de datos y a regular los elementos esenciales que definen este derecho. La propia naturaleza del RGPD (norma de alcance general, directamente aplicable y obligatoria en todos sus elementos) y la proscripción de toda norma nacional que lo reproduzca innecesariamente o que complete su contenido obstaculizando su efecto homoneizador en el conjunto de la Unión Europea convierten a la ley nacional que pretenda adaptar o completar dicha regulación en un producto normativo marginal.

El RGPD —no la ley orgánica— es la norma llamada a «desarrollar» el derecho fundamental consagrado en el art. 8 CDFUE y a regular sus «elementos esenciales» y lo ha hecho de forma muy exhaustiva al normar la práctica totalidad de los elementos conformadores de este derecho. Los 99 artículos del RGPD y los

173 Considerandos que los ilustran y completan conforman un marco normativo de cuya exhaustividad dan cuenta sus aproximadamente 65.000 palabras. Poco sentido tiene ya la recurrente doctrina constitucional que, desde el primer momento, advirtió de la necesidad de aplicar un criterio restrictivo en el desarrollo del derecho fundamental operado por la ley orgánica para evitar los riesgos de *petrificación* del ordenamiento (STC 5/1981) porque, sencillamente, el desarrollo del derecho fundamental de protección de datos lo opera el RGPD sin límite alguno sobre la materia regulada.

Muy poco debiera quedarle al legislador orgánico si observamos cómo la jurisprudencia europea obliga al legislador nacional a evitar reiteraciones innecesarias del RGPD limitándose a adoptar las previsiones a las que obligue el RGPD para su aplicación y a adaptarlo y completarlo atendiendo a las tradiciones jurídicas propias. El margen normativo del legislador orgánico es, aparentemente, mínimo. En consecuencia, ¿cómo explicar el abultado contenido final de la LOPDGDD? 85 artículos sobre protección de datos … Conforme al principio de autonomía institucional que informa el sistema multinivel europeo, la ley orgánica de protección de datos debiera restringir su alcance al «desarrollo directo y en sus elementos esenciales» del derecho fundamental de protección de datos, pero lo cierto es que la LOPDGDD extiende su objeto a aspectos bien específicos de la normativa de protección de datos sin que, en puridad, puedan considerarse todos ellos regulación de elementos básicos del derecho. Por el contrario, la naturaleza orgánica de la LOPDGDD no incluye la arquitectura institucional de garantía del derecho (AEPD y Autoridades autonómicas) cuando el art. 8 CDFUE eleva a categoría constitucional europea la exigencia de una autoridad independiente.

La conclusión es inevitable: la interpretación y aplicación del RGPD y la LOPDGDD constituye un reto mayúsculo. Su extensión, innovación terminológico-conceptual y el cambio de estrategia europea en la protección de datos abocan a dificultades hermenéuticas mucho más agravadas de las ya existentes bajo la videncia de la LOPD. Se trata de un paquete normativo integrado por sendos textos de amplio articulado aparentemente similar (99 artículos del RGPD por 97 de la LOPDGDD) cuyo correcto entendimiento obliga preceptivamente a su cotejo con el extenso Preámbulo de la LOPDGDD y los 173 Considerandos del RGPD: un total aproximado de 100.000 palabras. Además, esta nueva estrategia normativa de corte anglosajón adoptada por la Unión Europea contiene cambios significativos de naturaleza terminológica y conceptual que multiplican las dificultades hermenéuticas y el nuevo enfoque proactivo sobre el que se construye el cumplimiento de obligaciones derivadas del derecho de protección de datos aboca a una visión dúctil del sistema de protección que inevitablemente sólo resultará suficientemente completada mediante el ejercicio pleno de sus funciones por parte de las Autoridades de Control y los órganos jurisdiccionales. En definitiva, a los operadores jurídicos les espera una ardua tarea técnica que esperemos no vaya en detrimento de la garantía efectiva del derecho de protección de datos.

LUCRECIO REBOLLO DELGADO

Como he manifestado, la normativa de la UE ha sido pionera en materia de protección de datos y ha incentivado a regulaciones adecuadas de los Estados miembros, que han ido siguiendo las pautas marcadas, con mayor o menor fortuna, por la UE. Ninguna objeción puede realizarse en este ámbito, ni a los Estados miembros, ni a la UE. Quizás el problema provenga esencialmente de lo complejo de la materia. Esta circunstancia trae causa de tres elementos importantes: la complejidad tecnológica en la que se fundamentan las posibilidades; la celeridad de cambios y variaciones; y por último, y como no podría ser de otro manera, el uso generalizado de la tecnología por parte de los ciudadanos, y que como es propio de la condición humana, no siempre se utiliza de forma ajustada al bien común.

La sociedad digital emana en unas estructuras económicas y sociales, y en un Derecho producto de una evolución histórica. Bajo la pretensión inequívoca de solventar conflictos sociales, el Derecho tiene unos elementos consustanciales que plantean la duda de si son los adecuados para resolver los problemas sociales venideros y, singularmente, si será capaz de preservar los pilares de la ordenación social, de los que hoy disfrutamos: Estado de Derecho; la democracia; el desarrollo económico; y singularmente los derechos y libertades fundamentales. En ocasiones los desarrollos innovadores se han entremezclado con los procedimientos tradicionales, pero todo apunta a que la sociedad digital puede ser disruptiva con los mecanismos clásicos de ordenación social, y singularmente a través de la inteligencia artificial, puesto que sustraen al ser humano la capacidad de optar o decidir.

La subjetividad al respecto del planteamiento de este problema es muy variada. Hay quienes entienden que por mucha innovación tecnológica que se produzca, el ser humano seguirá conservando su singularidad y esencia, así como, en lo troncal, la sociedad quedará ordenada en parámetros similares a los actuales. Existe la postura que toma conciencia de la profundidad de los cambios ya existentes y venideros, pero no vislumbra peligro o problemática. Por último, existe una corriente de análisis que manifiesta una honda preocupación por los cambios tan radicales que puede introducir la sociedad digital, y que pueden ocasionar una desestructuración social.

Sin ser partícipe pleno de ninguna de las tres posturas referidas, parece claro que indefectiblemente habrá de ser el Derecho, entendido en una de sus acepciones más simples, como conjunto de normas, la herramienta que puede solventar la problemática que genere la sociedad digital. No es tarea sencilla, pero sí obligada del jurista, anticipar y ofrecer soluciones.

Son frecuentes las comparaciones de los datos con materias primas de mucho valor (petróleo, oro, diamantes) y podríamos manifestar con rotundidad que supera el valor de estos materiales, puesto que presentan características muy singularizadas:

— Los datos se producen en segundos y no se consumen, pueden ser reutilizados de forma indefinida.
— Son fáciles de registrar y almacenar, no requiriendo unas infraestructuras ni medios costosos.
— Su utilidad depende del tratamiento, pero éste es sumamente sencillo, cualquier ordenador personal actual puede efectuarlos.
— La inteligencia artificial y el Big Data pueden añadirle un valor incalculable e insospechado al tratamiento.
— Por último, el tratamiento no es perceptible, y generalmente se realiza en secreto. En unos casos con pretensión de beneficio empresarial, en otros por el poder que otorgan, y también porque en muchas ocasiones se realizan en un limbo jurídico.

El simple hecho de relacionar estas posibilidades debe poner en guardia a todo jurista, singularmente porque el ordenamiento jurídico, y el Estado, están muy alejados en la actualidad de poder regular en su integridad este *maremágnum*.

También parece claro que la nueva sociedad digital no puede ser ahormada o conformada únicamente por el Derecho, teniendo en cuenta que supone una nueva conformación horizontal del conjunto social, y que afecta a los medios de comunicación, a la economía, a todos los ámbitos de lo social, incluso a las mismas bases de organización social y política. Hoy es frecuente el uso del término holístico, para referir una afección a todos los elementos fundamentales que estructuran e informan nuestras sociedades. Por ello se hace obligatorio adoptar una perspectiva holística en el tratamiento de los retos que plantea la sociedad digital. Atribuir al Derecho la única forma de ordenar y encajar la sociedad digital es un grave error. El Derecho debe ser, como ha sido siempre, una forma de solventar conflictos sociales con una perspectiva de bien común.

Las soluciones existentes hasta ahora parecen de todo punto insuficientes. Hacemos repaso de las mismas. El Derecho internacional tiene una limitada capacidad coactiva, por su escasa vinculación y su menor entidad sancionadora. Su efectividad se limita a áreas muy concretas, como es el comercio a nivel mundial, algunos aspectos de propiedad intelectual y quizás con mayor eficacia, en materia de elaboración de tratados.

Otro ámbito en que de alguna forma se viene regulando la sociedad digital es el Derecho de defensa de la competencia. Las regulaciones nacionales encuentran grandes dificultades a la hora de la normación por la presión que ejercen de forma genérica las grandes empresas de tecnología, dado que aquélla siempre limita su capacidad de maniobra, a la vez que tienen múltiples formas de ir eludiendo las regulaciones nacionales. De igual manera, evitan con facilidad la competencia entre ellas, de tal manera que las denominadas «cinco grandes» (Google, Facebook, Microsoft, Amazon y Appel) se quedan con todo el mercado.

La única herramienta de control sobre las empresas tecnológicas hasta la fecha ha venido a través del derecho de la libre competencia. De esta forma, tanto algunos Estados europeos, como la propia Unión Europea, han impuesto sanciones económicas a Google, pero que han sido asumidas más como un coste añadido de producción, que como reproche jurídico efectivo a su actividad o a la forma de llevarla a efecto. En todo caso, el derecho de defensa de la competencia tiene como finalidad garantizar la funcionalidad de los mercados económicos y para impedir el abuso de una posición de dominio de mercado, pero no es un Derecho específico para limitar otros poderes (por ejemplo, políticos, culturales, sociales o de otra índole). El logro de objetivos de bien común como la protección de la autonomía (libertad frente a la manipulación), la equidad de oportunidades de acceso, la supresión de la discriminación o la formación de una opinión pública dirigida a la reproducción y promoción de la pluralidad social, no son objetivo específico del Derecho de defensa de la competencia.

Parece adecuado deducir que las soluciones que tiene que aportar el Derecho, han de venir de la extensión aplicativa de principios jurídicos a las nuevas necesidades sociales. Como nos recordara García de Enterría en sus *Reflexiones sobre la Ley y los principios generales del Derecho Administrativo*, «la ciencia jurídica no tiene otra misión que la de desvelar y descubrir a través de conexiones de sentido cada vez más profundas y ricas, mediante la construcción de instituciones y la integración respectiva de todas ellas en un conjunto, los principios generales sobre los que se articula y debe, por consiguiente, expresarse el orden jurídico. Este, en la sugerente expresión de Simonius, «está impregnado de principios hasta sus últimas ramificaciones», de modo que en hacer patente esa oculta y profunda vida de los principios está la augusta función del científico del Derecho, y no en ofrecer clasificaciones o sistematizaciones geométricas, lógicas o nemotécnicas de la materia de las leyes. Una ciencia jurídica puramente exegética (aunque quisiese incluir los «principios incluidos por el legislador en sus normas») no podría responder nunca a la clásica objeción de von Kirchmann: «tres palabras rectificadoras del legislador convierten bibliotecas enteras en basura»; el que esto no haya sido así y las obras de los grandes juristas de la historia no sólo no sean basura, sino que hayan adquirido un permanente y eficaz valor clásico, es justamente porque en ellas se ha acertado a expresar un orden institucional de principios jurídicos no sometidos a la usura del tiempo.

La superioridad del Derecho Romano sobre otros sistemas jurídicos históricos anteriores o posteriores estuvo justamente, no ya en la mayor perfección de sus leyes (acaso las de Licurgo, o las de cualquier otro de los grandes legisladores mitificados, fuesen superiores), sino en que sus juristas fueron los primeros que se adentraron en una jurisprudencia según principios, la cual ha acreditado su fecundidad, e incluso, paradójicamente, su perennidad, y hasta su superior certeza, frente a cualquier código perfecto y cerrado de todos los que la historia nos presenta».

La aportación que el jurista puede realizar a esta novedosa realidad social que denominamos sociedad digital, ha de venir, inexorablemente, precedida del

entendimiento del bagaje jurídico, que ha de cohonestarse con las nuevas necesidades. Ello ha de llevarse a efecto en base a la reconfiguración de principios jurídicos que nacen de una pretensión de ordenación social heredada, a la que se deben sumar las nuevas necesidades.

Pero este proceso no puede realizarse sin contextualización, ni ser el producto de un laboratorio aislado o desconocedor de las realidades sociales. Es una tarea de conjunto, y no menor. En definitiva, se trata de ir incardinando, a la vez que adecuando, el ordenamiento jurídico a las nuevas necesidades sociales. Para ello, es necesario el análisis concreto de los puntos jurídicos de mayor fricción o de superior dificultad de encaje, y de forma más concreta, los derechos y libertades fundamentales más expuestos a las innovaciones que provienen o generará el desarrollo tecnológico.

ANTONIO TRONCOSO REIGADA

Con la aprobación del RGPD el legislador europeo trata de garantizar el derecho fundamental a la protección de datos personales, mejorando la definición de su contenido, de sus facultades y de sus límites. Así, el RGPD avanza en el desarrollo de los principios de protección de datos personales y de los derechos de las personas en este ámbito, al mismo tiempo que ofrece una nueva configuración de las obligaciones de los responsables y de los encargados del tratamiento de datos personales y del papel de las autoridades de control. Todo ello va encaminado a que las personas tengan un mayor «poder de disposición y control» sobre sus datos personales sometidos a tratamiento, también en relación con los tratamientos transfronterizos, lo que «faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» —STC 292/2000, de 30 de noviembre, F. J. 7.º—.

Por todo ello el RGPD tiene que ser valorado, en términos generales, de manera positiva. El RGPD ofrece a las personas más instrumentos para el control sobre su información personal en la era de Internet, situando a la Unión Europea en una posición de equilibrio entre la libre circulación de la información personal y la tutela del derecho a la protección de datos personales. La posición adoptada en el RGPD ha sido especialmente acertada en este ámbito. Si como hemos señalado antes el incremento de los tratamientos de datos personales derivado del proceso tecnológico ha elevado los riesgos para la privacidad, el legislador europeo no se ha planteado limitar el recurso a las nuevas tecnologías e impedir las ventajas que éstas aportan a la empresa privada y a la Administración Pública sino que ha puesto el acento en que el progreso tecnológico imparable vaya acompasado a un proceso de fortalecimiento de las garantías del derecho a la protección de datos personales, que permitan a las personas un mayor control sobre sus datos personales sometidos a tratamiento.

El RGPD ha favorecido el control de las personas sobre sus datos personales, mejorando la regulación de los principios relativos al tratamiento de datos personales y de los derechos de las personas en este ámbito. Si bien, como señala el Considerando 9 del RGPD, los «principios de la Directiva 95/46/CE siguen siendo válidos», el RGPD hace un esfuerzo de concreción, definición y desarrollo de los principios ya incluidos en la Directiva. Así, el RGPD, al regular los principios relativos al tratamiento, junto con el principio de licitud y lealtad, proclama el principio de «transparencia de los tratamientos», que se concreta en la ampliación de la información al interesado y del derecho de acceso, el de «minimización de datos»; el de «limitación del plazo de conservación», y el «responsabilidad proactiva». Especial interés merece la regulación de la licitud de los tratamientos, especialmente relevante para nuestro país, al exigir para entenderse prestado el consentimiento una declaración o una clara acción afirmativa, lo que suprime el consentimiento tácito, y al reiterar como un supuesto de legitimidad del tratamiento que este sea necesario para la satisfacción de intereses legítimos por el responsable o por un tercero, siempre que no prevalezcan los intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, una previsión que ya se contenía en la Directiva 95/46/CE pero que no fue transpuesta en la legislación española y que añade un importante elemento de ponderación del que carecía nuestro ordenamiento jurídico de protección de datos. Igualmente, el RGPD fortalece los derechos del interesado, desarrollando el contenido de las facultades tradicionales y añadiendo nuevos derechos, de forma que ya no se puede hablar más de derechos *arco*. La información al interesado dentro del RGPD no es sólo un principio sino que es un derecho, agregando una información adicional al interesado que no se encontraba en la Directiva, como la relativa a la base jurídica del tratamiento, al delegado de protección de datos, al plazo de conservación de los datos, al derecho a retirar el consentimiento o al derecho a presentar una reclamación a la autoridad de control, incorporando el uso de iconos o la información por capas para garantizar que el incremento de la información al interesado no perjudique la transparencia del tratamiento de datos, mejorando la comprensibilidad y la accesibilidad de los tratamientos, especialmente en el caso de los menores. Igualmente se amplía el contenido del derecho de acceso del interesado con la información del plazo previsto de conservación de los datos o de la existencia de un derecho a solicitar del responsable información sobre el ejercicio de los derechos que asisten al interesado, entre otros. También se fortalece la regulación del derecho de rectificación, del derecho de supresión o derecho al olvido, del derecho de oposición y del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, al mismo tiempo que se reconocen nuevos derechos al interesado que no se encontraban en la Directiva 95/46/CE ni en la LOPD como el derecho a la limitación del tratamiento o el derecho a la portabilidad de los datos.

Uno de los objetivos del RGPD es hacer más sencillo y comprensible a los responsables y encargados de tratamiento el cumplimiento de la normativa de

protección de datos, incrementando al mismo tiempo su responsabilidad —la *accountability*— y, en general, el respeto a este derecho fundamental. Esto lo hace el legislador europeo: primero, suprimiendo algunas obligaciones de los responsables y encargados de tratamiento que eran consideradas burocráticas y poco útiles para la tutela del derecho fundamental; segundo, estableciendo unas obligaciones específicas a categorías concretas de responsables y encargados de tratamiento —y no a todos ellos de manera indiferenciada—; y tercero, añadiendo nuevas obligaciones de los responsables y encargados de tratamiento menos formales y más efectivas para la protección de datos personales.

Así, en primer lugar, el RGPD supone la supresión o la flexibilización de algunas exigencias recogidas en la LOPD como la obligación que tenían todos los responsables de notificación de todos los tratamientos de datos personales a la autoridad de control, lo que permitía la existencia de un derecho a la consulta al Registro General de Protección de Datos y que ha sido sustituida por un registro de las actividades de tratamiento, que es una medida de carácter interno. También han desaparecido algunas autorizaciones administrativas para las transferencias internacionales de datos, al ampliar los instrumentos de garantía que no requieren autorización al igual que se ha suprimido la obligación de cumplir un listado muy amplio de medidas de seguridad de carácter organizativo o técnico aprobadas por vía reglamentaria. De esta forma, el RGPD trata de desburocratizar la protección de datos personales, que en muchas ocasiones se había convertido para muchas empresas en un cumplimiento formal y vacío de algunas exigencias que se encomendaba a las gestorías y que se materializaba en la notificación de un tratamiento, en la existencia de un documento de seguridad estándar no adaptado a la organización o en la inclusión de unas cláusulas informativas genéricas.

En segundo lugar, el RGPD ha evitado establecer el mismo catálogo de obligaciones generales para cualquier clase de responsable o encargado del tratamiento, sino que ha fijado algunas obligaciones específicas a determinadas categorías de responsables y encargados de tratamiento, teniendo en cuenta la naturaleza de los tratamientos y los riesgos para los derechos de las personas. Así, si la obligación de notificación de todos los tratamientos a la autoridad de control era visto por las pequeñas y medianas empresas como una carga burocrática, el registro de actividades de tratamiento —que es la nueva obligación del RGPD que sustituye a la notificación— no se aplica a las empresas u organizaciones que empleen menos de doscientas cincuenta personas, salvo que el tratamiento pueda entrañar un riesgo para los derechos, no sea ocasional o incluya categorías especiales de datos personales o datos relativos a condenas o infracciones penales. Algo semejante puede decirse de la obligación de realizar una evaluación de impacto en la protección de datos o de designar un delegado de protección de datos que sólo se aplica a determinadas categorías de responsables o a tratamientos que por su naturaleza entrañen alto riesgo para los derechos de las personas. Tanto la supresión de algunas obligaciones como el establecimiento de otras sólo

para categorías concretas de responsables y encargados de tratamiento, poniendo el acento en dónde está realmente el riesgo y no en todas las pymes, ha simplificado en términos generales las obligaciones de estos, en línea con la posición británica en el proceso de negociación del Reglamento —vuelve a ser un texto pre-*Brexit*—, que buscaba que el nuevo marco normativa europeo no sobrecargase —*not overburden*— a las empresas y permitiera el desarrollo y la innovación.

En tercer lugar, el RGPD introduce algunas nuevas obligaciones del responsable y del encargado como la evaluación de impacto relativa a la protección de datos, el delegado de protección datos y la protección de datos en el diseño o por defecto que son obligaciones de carácter menos formal y burocrático, pero mucho más efectivas para el cumplimiento del derecho a la protección de datos personales y que reflejan mejor el principio de responsabilidad proactiva y la *accountability.* De esta forma, el RGPD no se limita a suprimir algunas exigencias de la normativa de protección de datos que podían ser consideradas formales o propio de las gestorías, sino que introduce nuevas garantías para la protección de datos personales que provienen en muchas ocasiones de la cultura jurídica anglosajona y del ámbito de la autorregulación. La introducción de la *privacy impact assesment*, de la *privacy by design*, de la *privacy by default* y del *data protection officer* nos aproximan al modelo anglosajón de protección de datos. Estas nuevas medidas como la responsabilidad proactiva o las evaluaciones de impacto en la protección de datos personales no pueden ser llevadas a cabo por una gestoría —no se trata del cumplimiento formal de una serie de trámites— sino por una persona con unos conocimientos especializados del Derecho y la práctica en materia de protección de datos.

Si el RGPD es una norma obligatoria en todos sus elementos y directamente aplicable, que no requiere una norma nacional de transposición, es necesario preguntarse qué sentido tiene la aprobación en nuestro país de una nueva Ley Orgánica de Protección de Datos Personales. Hay que recordar que la Unión Europea eligió el Reglamento como norma de derecho derivado institucional en detrimento de aprobar otra Directiva como la 95/46/CE justamente porque trataba de mejorar la armonización normativa en este ámbito de la protección de datos personales, reduciendo las divergencias existentes entre las legislaciones de los Estado miembros que permitía la Directiva 95/46/CE y que daba lugar a una fragmentación normativa que perjudicaba el funcionamiento adecuado del mercado interior. Son dos las razones que justifican la aprobación de una ley nacional de protección de datos personales. La primera razón es que le corresponde al legislador nacional, como ha señalado el TJUE, por razones de seguridad jurídica, la labor de depurar el ordenamiento jurídico interno, derogando preceptos incompatibles con el RGPD, evitando a los responsables de tratamiento o las autoridades de control situaciones de incertidumbre que les obliguen a interpretar en cada caso si un precepto legal debe ser o no inaplicado por haber quedado desplazado al estar en contradicción con el RGPD o que el juez nacional se plantee la necesidad de presentar una cuestión prejudicial antes de inaplicar la ley interna.

De esta forma, no deben mantenerse en el ordenamiento jurídico interno normas nacionales contrarias al RGPD aunque los poderes públicos procedan a la inaplicación. Lo mismo cabe decir de la legislación autonómica de protección de datos personales. La segunda razón es que el RGPD, a pesar de tener un alto nivel de detalle y de especificación —tiene 99 artículos y 173 considerandos—, a diferencia de otros Reglamentos de la Unión Europea, deja un margen de maniobra a los Estados para su desarrollo o complemento cuando el tratamiento de datos personales afecta a derechos constitucionales y a las categorías especiales de datos personales, para fijar de manera más precisa requisitos y otras medidas adicionales que garanticen un tratamiento lícito y equitativo en determinados ámbitos específicos o para regular los principios y derechos de protección de datos personales. El RGPD, aunque pueda parecer extraño, está llamando de alguna manera a la intervención legislativa de los Estados miembros para que concrete algunos ámbitos dejados a la decisión de los Estados. Así, el RGPD permite que sus disposiciones sean especificadas o restringidas por el Derecho de los Estados miembros, «conteniendo un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias». Muchos de los poderes que la Propuesta de Reglamento de la Comisión atribuía a la propia Comisión para hacer actos delegados y de ejecución han pasado en el texto finalmente aprobado a los Estados o han desaparecido. Como ya adelantábamos cuando se dio a conocer la Propuesta de Reglamento de la Comisión en 2012, «cuando avance el proceso negociador y crezca en los Gobiernos la preocupación por la pérdida neta de soberanía —o, al menos, la perciban— en un punto que afecta al desarrollo legislativo de un derecho fundamental, posiblemente la propuesta de Reglamento comience a incluir más habilitaciones a los Estados, concediéndoles a éstos un mayor margen de apreciación, de manera que se pase de una Directiva —la 95/46/CE— que permitía una flexibilidad formal a un Reglamento que sea flexible en lo material. En todo caso, cualquiera que sea la mayor o menor flexibilidad material del Reglamento, lo que está claro es que su aprobación va a reducir la libertad del legislador nacional en el desarrollo de un derecho fundamental y afecta al principio democrático».

El RGPD estableció un plazo de dos años a partir de la fecha de la entrada en vigor para el inicio de su aplicación, que finalizó el 25 de mayo de 2018, lo que se debió principalmente a que, siendo el derecho un importante instrumento de ingeniería social, la realidad no cambia sólo porque el derecho cambie. Era necesario un periodo de tiempo para el conocimiento y la adaptación tanto de las Administraciones Públicas como de las empresas privadas al nuevo derecho derivado institucional de la Unión Europea. El RGPD introducía no sólo un gran número de novedades en relación con la Directiva 95/46/CE y con la legislación vigente en los Estados miembros sino que suponía, en gran medida, un cambio de enfoque. Hacía falta tiempo para adecuar los ordenamientos jurídicos de los Estados miembros a los cambios establecidos en el RGPD que hace descansar en gran medida el cumplimiento de la normativa de protección de datos personales en la

responsabilidad proactiva y en la autorregulación. En todo caso, hay que poner de manifiesto que el Gobierno apuró excesivamente el plazo para ejercer la iniciativa legislativa que permitiera adaptar la legislación interna que había transpuesto la ya derogada Directiva 95/46/CE al nuevo derecho derivado institucional de la Unión Europea por lo que el RGPD inició su aplicación sin haberse aprobado todavía la LOPDGDD. Esto se evidencia aún más teniendo en cuenta que la Propuesta de Reglamento fue aprobada por la Comisión en enero de 2012 y tuvo una tramitación muy lenta en las instituciones europeas, interviniendo el Gobierno en el procedimiento legislativo por lo que había dispuesto de la información y del tiempo suficiente para haber elaborado con anterioridad el anteproyecto.

La LOPDGDD, a diferencia del RGPD, tiene un objeto más amplio porque trata de garantizar los derechos digitales de la ciudadanía más allá del derecho fundamental a la protección de datos personales, lo que también se manifiesta en su «Ámbito de aplicación material», que no se circunscribe a los tratamientos de datos personales en el caso del Título X «Garantía de los derechos digitales», salvo los artículos 89 al 94 para los que sí se exige el tratamiento de datos personales. El carácter más amplio de la LOPDGDD en relación con el RGPD se pone de manifiesto en el propio título. Si el Reglamento es «relativo a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos, la Ley Orgánica 3/2018, de 5 de diciembre no es sólo de Protección de Datos Personales sino también de garantía de los derechos digitales. Fueron las Cortes Generales, también a través del trámite de enmiendas, quienes subrayaron la importancia de garantizar en esta Ley el pleno ejercicio de los derechos fundamentales en Internet, algo que se plantea como la antesala de una futura reforma constitucional que reconozca y dé rango constitucional a los derechos digitales de los ciudadanos y que actualice la Constitución a la era digital.

La LOPDGDD posibilita las iniciativas en el ámbito de la salud pública y de la investigación sanitaria. Inicialmente se podía afirmar que la aprobación del RGPD facilitaba la investigación sanitaria, especialmente en nuestro país que tenía un marco jurídico muy restrictivo en este ámbito, sin perjuicio de que el RGPD pudiera haber sido más preciso. Sin embargo, aprobado el RGPD se había discutido en algunos foros si esta cuestión había quedado suficientemente clara en el RGPD y si suponía realmente un cambio en el régimen jurídico vigente de la investigación sanitaria en nuestro país. Pues bien, el PLOPD aprobado por el Consejo de Ministro no se refería a esta cuestión. Fueron las enmiendas de los Grupos Parlamentarios, que fueron sensibles al planteamiento de los grupos de investigación y de la industria, los que permitieron incorporar al Proyecto una nueva DA 17.ª, que lleva por título «Tratamientos de datos de salud» y que aporta una mayor seguridad jurídica en este ámbito, interpretando el consentimiento explícito no para una concreta investigación sino para áreas generales vinculadas a especialidades médicas e investigadoras y permitiendo los tratamientos de datos seudonimizados sin consentimiento del interesado con fines de investigación en salud y en particular biomédica, con

garantías adicionales de información y con el informe previo del comité de ética de la investigación, entre otras salvaguardas.

Por último no hay que olvidar que corresponde al Consejo de Ministros la aprobación del proyecto de Ley para la transposición de la Directiva (UE) 2016/680 y su remisión a las Cortes Generales. El Estado Español ha incumplido el plazo de transposición, que finalizó el 6 de mayo de 2018. En cambio Alemania ya aprobó la Ley de adaptación de la Ley de protección de datos al Reglamento (UE) 2016/679 y de aplicación de la Directiva (UE) 2016/680 (Ley de protección de datos —Ley de adaptación y aplicación de la UE, de 30 de junio de 2017). El Ministerio del Interior está trabajando en un Anteproyecto de Ley, excluyendo los tratamientos de datos personales del ámbito jurisdiccional, que ha pasado el trámite de consulta pública. El Ministerio de Justicia debe avanzar también en la modificación de la LOPJ que mejore los arts. 230 y ss, y las leyes procesales para adaptarlas al RGPD, a la Directiva 2016/680 y a la LOPDGDD. También le corresponde al Gobierno derogar la normativa reglamentaria incompatible con el Derecho de la Unión Europea, en especial el Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

6. *En esta materia se han creado organismos independientes de garantía, como la Agencia Española de Protección de Datos ¿qué valoración le merece el régimen jurídico que se le ha dado? ¿Cree que sería necesaria o conveniente alguna modificación en su régimen jurídico o en algún otro aspecto del sistema de garantías de este derecho?*

LORENZO COTINO HUESO

La protección de datos ha incluido desde su inicio una dimensión institucional con la protección específica a través de autoridades independientes, sin perjuicio de la garantía judicial. En general se ha demostrado como un instrumento eficaz para una mejor protección del derecho y ha permitido un acervo y especialización importante. De igual modo la coordinación y cooperación con las autoridades de protección de datos de los Estados y de la UE (Grupo del 29, Comité Europeo de Protección de Datos) ha generado un valioso conocimiento y *soft law*. Los sucesivos directores o directoras de las autoridades independientes en España —en especial, la AEPD— han dejado su respectiva impronta. Por lo general, los nombramientos han sido de perfiles políticos. Ello, que en general es negativo, no ha impedido un nivel adecuado y una independencia en su actuación. Pese a que las autoridades independientes han ido creciendo en recursos y personal, no lo han hecho al ritmo de las necesidades de un sector y un crecimiento casi exponencial de peligros y riesgos. Tanto las autoridades como los tribunales europeos han intentado marcar el territorio a las grandes tecnológicas y plataformas. La actual regulación parece en general adecuada e incluso refuerza algo más la independencia de las autoridades

que hay en España. Va a ser importante ver cómo se articulan los mecanismos de cooperación y cohesión entre las autoridades europeas, pues es un régimen bastante complejo.

El cambio hacia el modelo de responsabilidad proactiva que deje atrás un modelo burocrático y bastante inútil es sin duda un especial reto en España. Ello ha de llevar a las autoridades independientes a poner más énfasis en las garantías reales de la protección de datos.

Frente a los grandes impactos por la inteligencia artificial y otras tecnologías disruptivas no está aún claro el modelo de garantías a seguir. Muy posiblemente las autoridades independientes de protección de datos van a ganar más competencias, extendiéndose también a la lucha frente a la discriminación y sesgo algorítmicos. De igual modo es posible que surjan nuevas autoridades especializadas para el control del cumplimiento normativo de la inteligencia artificial, como el sistema de aprobación previa de los sistemas que impliquen un alto riesgo (Libro blanco de la Comisión Europea de febrero de 2020). Asimismo, es muy posible que autoridades de control de diversos sectores extiendan su ámbito de actuación a temas de automatización e inteligencia artificial (comunicaciones, salud, bioética, sector público específico, Derecho de la competencia, autoridades electorales, audiovisuales, etc.).

Es necesario que los diversos órganos de garantía integren técnicos, juristas y especialistas en ética y pasen a modelos dinámicos de evaluación de riesgos con fórmulas regulatorias flexibles. De igual modo la sociedad civil es importante que esté presente, especialmente frente a los impactos colectivos y bienes públicos de las tecnologías disruptivas que quedan, según se ha dicho, muchas veces a la sombra del derecho subjetivo de protección de datos.

ROSARIO GARCÍA MAHAMUT

Una de las grandes aportaciones del RGPD reside en la ruptura del principio de territorialidad a favor de la homogeneización normativa. Ello se halla en íntima conexión con la regulación que el RGPD establece de las autoridades de control (art. 51), su independencia (art. 52) y sus funciones (art. 57); con los procedimientos previstos en caso de vulneración de la normativa de protección de datos; y el modelo de ventanilla única con una autoridad de control principal y el procedimiento de cooperación entre autoridades, donde la decisión vinculante el Comité Europeo de Protección de Datos resultan absolutamente relevantes para el sistema de garantías.

En principio, el régimen previsto en la LOPDGDD para la AEPD cumple lo que mandata el RGPD, antes incluso de algunas de las previsiones hoy directamente aplicables por los distintos Estados miembros dada la naturaleza del RGPD. La efectiva aplicación del RGPD ha supuesto que la AEPD haya potenciado la implementación y publicación de nuevas herramientas, guías y documentos que

aseguren el cumplimiento de la normativa de protección de datos de forma proactiva o preventiva.

Ahora bien, no es menos cierto que hoy frente a conflictos concretos de incomparable envergadura lo más llamativo, a mi juicio, es el papel poco incisivo que ha desempeñado la AEPD con respecto al tratamiento de datos durante el estado de alarma por la crisis sanitaria de la COVID-19. Especialmente si tenemos en cuenta que, entre otras muchas consideraciones, la LOPDGDD aporta alguna luz en el tratamiento de los datos de salud —también con fines de investigación— epicentro de muchos de los debates y herramientas que se utilizan y se prevén utilizar para la protección de la salud y la prevención de los contagios. No obstante, también debe ponerse en valor que durante este tiempo la AEPD ha publicado distintos estudios de interés, ha respondido a distintas consultas sobre cuestiones relativas al uso de técnicas de reconocimiento facial o ha publicado una serie de recomendaciones para proteger los datos personales.

El tiempo dirá, pero me temo que el impacto de los instrumentos tecnológicos puestos a disposición de la lucha contra la pandemia seguirá demandando evaluación, seguimiento, revisión y posicionamiento claro tanto de las autoridades nacionales como de las comunitarias y ello conllevará modificaciones concretas del régimen de garantías.

PABLO LUCAS MURILLO DE LA CUEVA

Ha sido una pauta común en los ordenamientos contemporáneos dotar al régimen jurídico dedicado a la protección de los datos personales de un órgano especializado que, desde una posición de autonomía, ofrece una primera línea de defensa al derecho fundamental. Ya se ha visto que el Reglamento (UE) 2016/679 encomienda a las autoridades nacionales de protección de datos y al Comité Europeo de Protección de Datos la misión de hacer efectivas sus previsiones. Ya antes, el Consejo de Europa añadió el Protocolo Adicional n.º 181, de 8 de noviembre de 2001, al Convenio 108 para incluir entre los elementos necesarios para la adecuada protección de los datos personales a las autoridades de control.

En España la LORTAD optó por el modelo monocrático en vez de por el colegiado y creó la Agencia de Protección de Datos, años más tarde, ya bajo la LOPD, apellidada Española para distinguirla de las creadas por las Comunidades Autónomas. Sus primeros responsables supieron asentarla con rapidez y desde sus primeros pasos se ha distinguido por la seriedad de su actuación. Se pueden advertir distintas etapas en su trayectoria, algunas claramente más activas que otras en las que alcanzó, además, una notable proyección europea e internacional, pero lo importante es que está consolidada y ha hecho un buen trabajo desde que se constituyó en 1994, entre otras razones gracias a la continuidad de buena parte de sus técnicos. Un buen indicador de su acierto es que la mayor parte de sus decisiones objeto de recurso han sido confirmadas por los tribunales.

Con el Reglamento (UE) 2016/679 afronta retos de enorme calado y bien complicados, dada la complejidad de los mecanismos en él previstos y la vasta tarea que le corresponde. No me parece que para hacerles frente precise de modificaciones normativas pero sí, como decía antes, de los medios necesarios para desempeñar de la manera más eficiente su cometido. Y, si su situación en ese aspecto responde a la tónica que se advierte en otros ámbitos del sector público, me temo que no cuente con los suficientes.

MANUEL MEDINA GUERRERO

Como apuntamos líneas arriba, la existencia de un órgano independiente de control constituye, desde la Directiva, un elemento central del régimen de tutela del derecho a la protección de datos. Los principales cambios introducidos por la nueva LOPD inciden en el órgano unipersonal decisorio de la AEPD. Además de la ampliación del mandato (de cuatro a cinco años), hay una modificación sustancial del procedimiento de designación: si en el anterior sistema la Dirección la elegía el Gobierno entre los componentes del Consejo Consultivo, ahora el mecanismo es más complejo: convocatoria pública de candidatos; propuesta de Presidencia y Adjunto que remite el Gobierno al Congreso de los Diputados; ratificación por la Comisión de Justicia por mayoría de tres quintos, o por mayoría absoluta en una segunda votación siempre y cuando sea respaldada por diputados de dos grupos parlamentarios diferentes.

Aunque es de justicia notar la acreditada imparcialidad mostrada en su gestión por los titulares de la Dirección elegidos bajo el anterior sistema, creo que el nuevo diseño institucional presenta la gran ventaja de robustecer la imparcialidad de la institución al requerir su nombramiento el apoyo parlamentario. De hecho, la incorporación del Congreso de los Diputados resultaba poco menos que obligada desde el momento en que se constituyó el Consejo de Transparencia y Buen Gobierno, cuyo Presidente es nombrado previo acuerdo por mayoría absoluta de la Comisión correspondiente del Congreso. Resulta lógica la equiparación del sistema de elección de dos instituciones que, a la vista de sus funciones, parecen llamadas a entrar ocasionalmente en conflicto.

También debe valorarse positivamente la ampliación del mandato de cuatro a cinco años, asumiéndose así también el precedente del Consejo de Transparencia, al evitarse su coincidencia con la duración de las legislaturas parlamentarias.

ARTEMI RALLO LOMBARTE

El régimen jurídico de la AEPD no ha sufrido un impacto significativo por el nuevo marco normativo europeo (RGPD). Más bien al contrario, pudiera

pensarse que el modelo de Autoridades de control consagrado en el RGPD tomó como referencia a España en las nuevas funciones y potestades sancionatorias que otorga a las APDs. Ahora bien, con resultar globalmente satisfactorio su funcionamiento, la AEPD adolece de debilidades que merecen señalarse.

Las Autoridades de Protección de Datos tienen un reto mayúsculo que difícilmente podrán alcanzar con sus pautas actuales de funcionamiento: anticiparse a la ingente problemática y a los innumerables riesgos que se ciernen sobre el derecho de protección de datos de los ciudadanos. Anticiparse para evitar riesgos e infracciones. Pero anticiparse exige medios y habilitaciones que hoy posiblemente no existen o escasean. Las APDs han sido incapaces, hasta la fecha, de dotarse de herramientas tecnológicas y recursos humanos suficientes para afrontar un análisis exigente, riguroso y avanzado de los innumerables productos tecnológicos que emergen en el mercado. Como mucho, las APDs están en condiciones de realizar un «muestreo» sobre los peligros tecnológicos existentes pero, más allá de su valor tendencial o estadístico, eso no resulta suficientemente satisfactorio. Además, las habilitaciones legales para intervenir profilácticamente en el mercado tecnológico no resultan suficientes. El marco institucional y normativo existente proclama principios (privacy by design and by default) que «deben» cumplirse por los responsables de tratamientos de datos y, caso de no poder demostrar su cumplimiento, imponer una reacción punitiva. No es suficiente. Las APDs deberían realizar una fiscalización previa efectiva: una especie de homologación previa en privacidad y protección de datos. Pero, para ello, serían necesarios muchos medios humanos y materiales y un marco normativo que les atribuyera esa capacidad.

El RGPD ha tenido un gran impacto socio-mediático y ha fortalecido notablemente la visibilidad de la protección de datos y, en consecuencia, la concienciación social de este derecho. Esa es una realidad viva y creciente. Sin embargo, al mismo tiempo, el RGPD ha debilitado las estrategias represivas anteponiendo o beneficiando las reglas preventivas articuladas en torno a la «accountability». Existe una duda razonable de que este modelo de origen anglosajón vaya a funcionar en plenitud en la cultura jurídica continental europea y, en particular, en España. Para su funcionamiento hay que reforzar el vínculo y la relación AEPD-responsables (esto es, empresas, organizaciones, Administraciones públicas, etc.) de forma directa o a través de los Delegados de Protección de Datos. Hay que mantener una relación eficiente y exigente y no meramente aparente, formal u ornamental. Este esfuerzo adicional de la AEPD debe acompañarse adicionalmente de una capacidad efectiva de instruir y ordenar a empresas y entidades en el cumplimiento real de la normativa: llamémoslo un «enforcement preventivo». El principal riesgo actual de la AEPD es el de convertirse en lo que durante décadas tanto criticó en sus homólogas europeas faltas de habilitaciones legales que les permitieran garantizar efectivamente el derecho de protección de datos derivando a una estrategia proactiva de muy dudosos resultados.

LUCRECIO REBOLLO DELGADO

El reconocimiento histórico de los derechos nos muestra con gran claridad que la mera inserción de éstos en normas, sean del rango que sean, no supone su vigencia efectiva. Para asegurar el cumplimiento y respeto de los derechos todos los ordenamientos jurídicos han instituido elementos de garantía. De esta forma se suelen establecer en la doctrina tres tipos o medios de promover la plena vigencia de los derechos: las garantías normativas; los procedimientos jurídicos específicos, que suelen caracterizarse por su simplicidad y celeridad jurídica; y por último las denominadas garantías institucionales, habiéndose demostrado que son éstas en grado sustantivo esenciales en la vigencia de los derechos, tanto por su carácter coactivo como por la labor divulgativa que realizan de los derechos, así como por su especialización en un área concreta. A este objetivo contribuyó por vez primera la LORTAD en 1992, con la creación de la entonces Agencia de Protección de Datos, que la LOPD convirtió en Agencia Española de Protección de Datos y que facilitó la creación de instituciones similares en las CC.AA. aunque en la actualidad únicamente existan las de Cataluña y País Vasco. A ello se suma el Supervisor Europeo de Protección de Datos. En conjunto, estas denominadas autoridades de control realizan una actividad esencial en la vigencia del derecho a la protección de datos de carácter personal, dado que junto a las funciones clásicas de toda Administración pública y su actividad ejecutiva y coactiva, realizan una labor de divulgación muy necesaria, dado el uso masivo de las nuevas tecnologías por la sociedad.

En cuanto a su valoración, si bien es innegable la justificación de su existencia, no es menos cierto que su eficacia se ha visto mediatizada por el escaso impulso político que le es necesario para su plena virtualidad, si bien es cierto que esta deficiencia se aprecia con menor intensidad en la Unión Europea que en algunos Estados miembros. Para paliar esta deficiencia sería deseable equiparar en ejecutividad de control, a través de mecanismos jurídicos, a las autoridades de control de los Estados con la institución del Defensor del Pueblo (*Ombudsman*) lo que le daría una mayor virtualidad, y eficacia a sus funciones.

Otro aspecto esencial, y del que la configuración realizada por la LO 3/2018 deja camino para mejorar, es hacer a las autoridades de control mucho más permeables a las demandas de la multiplicidad de asociaciones particulares existentes, puesto que ellas son las canalizadoras de las demandas y necesidades sociales. Esta previsión que de forma muy lacónica se pretende introducir con la citada ley a través del Consejo Consultivo de la AEPD, no se ha articulado ni previsto de forma adecuada, lo que supone un lastre importante para la efectividad de sus objetivos.

Por último, y aunque no es únicamente imputable a las autoridades de control, y sí extensible a todos los organismos públicos y ciudadanos, existe una perspectiva algo anacrónica del derecho a la protección de datos de carácter personal y de forma más genérica de todo lo relacionado con el Derecho y la sociedad

digital, que debemos ir variando. La regulación jurídica de las nuevas tecnologías ha venido para quedarse, a la vez que ha adquirido una importancia social capital. Ya no se trata de simples requisitos que debemos cumplir más o menos formalmente, es una necesidad social asimilar sus postulados e insertar su vigencia de forma coherente en nuestra ordenación social, porque en ello nos va la continuidad de una ordenación social basada en el bien común.

ANTONIO TRONCOSO REIGADA

El RGPD fortalece a las autoridades de control en sus funciones y en la posibilidad de imponer importantes sanciones económicas, de manera que puedan ser eficaces en la supervisión y la aplicación de la normativa de protección de datos, unificando su capacidad coercitiva y estableciendo mecanismos que faciliten una aplicación coherente de la protección de datos personales en toda la Unión Europea. Este planteamiento trata de dar respuesta a las diferencias en el derecho a la protección de datos personales en los diferentes países miembros que provenían también, como hemos indicado antes, de las divergencias de las autoridades de control ante el mismo supuesto de hecho y de los déficits de *enforcement* en la aplicación de la normativa de protección de datos personales por los diferentes Estados. Por eso, el RGPD supone, de alguna manera, un reconocimiento implícito del modelo español de protección de datos personales y de la actividad de supervisión y control que ha desempeñado la Agencia Española de Protección de Datos en las últimas dos décadas.

El RGPD dedica una considerable atención a la independencia de las autoridades de control. Esto significa que es un aspecto que inquieta al legislador europeo. La Comisión había manifestado en el Segundo Informe de aplicación de la Directiva que «una preocupación es el respeto por el requisito de que las autoridades supervisoras de protección de datos actúen con total independencia». Por ello, el RGPD, recoge que el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un *elemento esencial* para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal. Tanto el art. 8.3 de la CDFUE como el art. 16.2 TFUE subrayan que el respeto a las normas de protección de datos personales debe estar sujeto al control de una autoridad independiente.

Por ello, el RGPD no se limita a proclamar de manera genérica la independencia de las autoridades de control sino que refuerza su independencia, exigiendo que cada Estado miembro atribuya a su autoridad de control un conjunto de garantías formales y sustanciales de independencia, recogiendo la jurisprudencia del TJUE a estos efectos y tratando de evitar que el Gobierno influya directa o indirectamente en las decisiones de las autoridad de control o que éstas no sean capaces de actuar de forma objetiva al interpretar la normativa. Muchas de estas

cuestiones se encontraban razonablemente resueltas en la legislación española pero no tanto en la de todos los Estados de la Unión. El RGPD supone un importante avance en la atribución a las autoridades de control de unas garantías formales de independencia, que no estaban presentes en la Directiva y que se pueden clasificar en dos: garantías relativas a los miembros de la autoridad de control, como son la forma y requisitos para el nombramiento, la duración del mandato, la inamovilidad y la incompatibilidad, y que configuran un auténtico estatuto jurídico de los miembros de las autoridades de control; y garantías relativas al funcionamiento de la propia autoridad de control, como son la autonomía de personal, presupuestaria y financiera y la disponibilidad de recursos humanos y económicos para el cumplimiento de sus funciones. En este punto el RGPD debe ser interpretado como un texto que trata de avanzar en las garantías formales de independencia de las autoridades de control, con el límite de no afectar al principio de autonomía institucional y a la soberanía de los Estados.

El RGPD recoge los requisitos para el nombramiento de miembro de la autoridad de control, señalando que «cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes». Existen, por tanto, «unas cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de una autoridad de control». La LOPDGDD prevé que el nombramiento del Presidente y del adjunto recaiga entre personas de «reconocida competencia profesional, en particular en materia de protección de datos». Evidentemente se trata de un ámbito donde existe un amplio margen de discrecionalidad y de apreciación a la hora de valorar si un candidato posee la cualificación y la idoneidad para ser nombrado, lo que limita el control jurisdiccional pero éste debe ejercerse en los supuestos en los que de manera clara y manifiesta el candidato propuesto no posee la titulación y la experiencia necesaria en el ámbito de la protección de datos personales, elementos éstos más reglados que la mayor o menor aptitud de un candidato que es siempre difícilmente valorable. También es importante subrayar la incompatibilidad y el deber de que los miembros de la autoridad de control actúen con integridad y discreción en lo que respecta a la aceptación de cargos y beneficios, una referencia genérica que trata de evitar la captura de las autoridades por intereses privados. Un elemento necesario tanto para la independencia de las autoridades de control como para el correcto cumplimiento de sus funciones es que éstas cuenten con los medios humanos, técnicos, financieros y organizativos para poder ejercer sus poderes. Hay que evitar que los Estados aprovechen el contexto de crisis económica para debilitar a las autoridades de control, especialmente en el ámbito de las Comunidades Autónomas, al ser estas los órganos garantes del derecho fundamental en los tratamientos de datos personales que llevan a cabo las Administraciones Públicas de este ámbito territorial.

Uno de los desafíos que tiene las autoridades de control en los próximos años es aplicar el RGPD y la LOPDGDD en un contexto de crisis económica y de

grave problema de salud pública por la pandemia del Coronavirus. El tratamiento de datos personales en el ámbito de la salud pública y de la investigación sanitaria sin consentimiento del interesado dispone en el RGPD y la LOPDGD de suficientes habilitaciones normativas y de garantías. La situación de grave crisis económica y las necesidades de creación de empleo obligan a interiorizar bien el doble objetivo del nuevo marco normativo europeo al que antes nos hemos referido y que no se limita a la protección de datos personales, sino que se extiende también a favorecer la libre circulación de datos personales que permita el crecimiento de la economía digital. Además, las autoridades de control deben garantizar el derecho fundamental a la protección de datos personales también en el contexto de los avances de las TIC antes mencionados —*Big Data*, inteligencia artificial, *Machine Learning,* etc.—. Por ello, dentro de la promoción del derecho fundamental es una importante prioridad hacer un seguimiento del desarrollo de las tecnologías de la información y de su incidencia en el derecho a la protección de datos personales, llevando a cabo una evaluación de los riesgos y de las garantías necesarias para la protección de datos personales y que vaya dirigida tanto a responsables y encargados de tratamiento como a ciudadanos. Esta es una función que desarrolla desde hace años la Unidad de Evaluación y Estudios Tecnológicos de la AEPD, que debe ser contemplada en el futuro Estatuto de la APDCM, al mismo tiempo que desaparece orgánicamente el registro de ficheros como subdirección general. Posiblemente en una situación de emergencia sanitaria como la actual, sin perjuicio de que la protección de datos personales desde el diseño sea una obligación del responsable del tratamiento y no de la autoridad de control, es importante la implicación de las autoridades de control para ayudar a la puesta en marcha de iniciativas tecnológicas que lleven a cabo tratamientos de datos personales para algunas finalidades de salud —por ejemplo, las *apps* que permiten el rastreo de los contactos y las cesiones de datos de localización o la inteligencia artificial aplicada a la historias clínica electrónica—, al mismo tiempo que respetan la normativa de protección de datos personales. Posiblemente las autoridades de control tienen que impulsar una labor de consultoría y de apoyo a los responsables de tratamiento como la que en el pasado desarrolló la APD de la Comunidad de Madrid.

Si bien le corresponde al responsable del tratamiento y no a la autoridad de control, en virtud del principio de responsabilidad proactiva, cumplir lo dispuesto en el RGPD y ser capaz de demostrarlo, aplicando las medidas técnicas y organizativas apropiadas 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, no obstante, las autoridades de protección de datos deben desarrollar una actividad prestacional o de promoción positiva del derecho fundamental a la protección de datos personales. Por tanto, las autoridades de control no se deben limitar a una función preventiva —de control previo o *prior checking*— o tuitiva, sino que deben desplegar una actividad de consultoría y de asesoramiento jurídico

que está orientada a que las Administraciones Publicas y empresas privadas se adecúen al derecho fundamental a la protección de datos personales. De esta forma, las autoridades de protección de datos deben impulsar una labor de garantía de este derecho fundamental, no sólo en su vertiente subjetiva como derecho frente al Estado —o frente a poderes privados— sino también en su vertiente objetiva o prestacional que implica una actividad pública de apoyo que haga del derecho fundamental a la protección de datos personales un derecho real y efectivo. Como ya señalamos en el pasado, le corresponde a las autoridades de protección de datos personales, de manera específica, una adecuación del derecho a la protección de datos personales en las Administraciones Públicas, interpretándolo de conformidad con otros derechos fundamentales y obligaciones constitucionales que exigen una actividad pública objetiva de prestación de los mismos a través de tratamientos de datos personales, de manera que las necesidades de la gestión pública se adecúen al derecho fundamental a la protección de datos personales. En esta dirección, hemos defendido siempre una aproximación equilibrada a la protección de datos personales, sin caer en el descreimiento, pero sin dar lugar tampoco al nacimiento de un nuevo fundamentalismo. Así, si la enorme injerencia y daño que se ha efectuado a los derechos fundamentales en la pandemia —al derecho a la vida y a la protección a la salud, a la libertad de movimientos, al derecho a la educación, al derecho al trabajo, a la libertad de empresa— se hubiera podido evitar con tratamientos de datos personales, era una obligación constitucional haberlo hecho así. Cualquier planteamiento que absolutice el derecho fundamental a la protección de datos personales sobre el resto de los derechos fundamentales vulnera el ordenamiento constitucional por no respetar el principio de proporcionalidad. La protección de datos personales es un derecho fundamental —no es una doctrina, no es una ideología— y debe interpretarse de conformidad con otros derechos fundamentales y valores constitucionales como la vida y la dignidad de la persona. Esto debe ser también interiorizado por las autoridades de control.

Una lógica preocupación es si el marco normativo común puede verse amenazado por la diversidad de criterios locales, que es consecuencia de diversos factores: la existencia de tratamientos locales que se producen en todos los Estados miembros —por ejemplo, la investigación sanitaria— o de tratamientos transfronterizos, es decir, de tratamientos realizados en establecimientos en más de un Estado miembro o que afecten sustancialmente a interesados en más de un Estado miembro. Lo importante no es que exista una diversidad inicial de criterios locales sino cómo se resuelve esta diversidad de manera que el ciudadano europeo tenga el mismo derecho a la protección de datos personales en el ámbito de la Unión Europea. Uno de los aspectos más innovadores del RGPD —y que supone una aportación muy notable para otros ámbitos distintos de la protección de datos personales— es la forma en que el RGPD ha resuelto la problemática de la diversidad de criterios locales, a través del funcionamiento de los mecanismos de cooperación y coherencia entre autoridades de protección de datos.

El Reglamento no sólo regula quién debe actuar como autoridad de control principal sino también la posición en la que quedan en los tratamientos transnacionales las autoridades de control del resto de los Estados miembros afectados por el tratamiento. El Reglamento no permite que la autoridad de control principal —la autoridad de control del establecimiento principal— actúe de manera independiente y con indiferencia a la posición del resto de las autoridades de control de los Estados miembros afectados por el tratamiento. La propia calificación de autoridades interesadas que hace el Reglamento de estas autoridades de control dice mucho de la posición que éstas pueden mantener en los tratamientos transnacionales. Así, la autoridad de control principal debe cooperar con las demás autoridades interesadas. Además, el RGPD establece unos mecanismos de cooperación y coherencia. Es también importante subrayar el importante papel del Comité Europeo de Protección de Datos para la formulación de directrices sobre cualquier cuestión relacionada con la aplicación del Reglamento.

Es esencial que el funcionamiento de los mecanismos de cooperación y coherencia y del Comité Europeo de Protección de Datos tenga en cuenta la arquitectura constitucional de Estados que son claramente descentralizados como es el caso de España, lo que requiere la participación de las autoridades subnacionales en los mecanismos de coherencia, también para limitar la diversidad de criterios locales a nivel nacional. Es necesaria una cooperación rápida y fluida con las autoridades de control a nivel nacional. En este punto existe una obligación recíproca: no sólo le corresponde a las autoridades subnacionales cumplir las normas relativas al mecanismo de coherencia y contribuir a la aplicación coherente del Reglamento en toda la Unión. También un Estado miembro con varias autoridades de control subnacionales debe garantizar la participación efectiva de estas en el mecanismo de coherencia, por lo que las autoridades subnacionales deben también colaborar en la toma de posición de la autoridad nacional en el Comité Europeo de Protección de Datos y en los mecanismos de coherencia. Por tanto, todas las autoridades, también las subnacionales, deben contribuir a la aplicación coherente del Reglamento en toda la Unión Europea, lo que les obliga a cooperar entre sí y con la Comisión. Esta obligación de cooperación tiene especial aplicación en las relaciones entre autoridades estatales y subestatales, teniendo en cuenta que deben interpretar y aplicar de manera coherente el Reglamento en el ámbito del ordenamiento jurídico interno.

CAMINO VIDAL FUEYO

En el 2020 se cumplen 27 años de la creación de la Agencia Española de Protección de Datos (AEPD) y a lo largo de este tiempo se ha convertido en un organismo que, en mi opinión, ha experimentado una progresiva mejora en lo que se refiere al contacto directo y cercano con los ciudadanos, con las empresas y con el denominado «sector de la economía digital».

No tengo formado un juicio crítico en relación con su régimen jurídico, pues entiendo que la sujeción de la Agencia al Derecho Administrativo, tanto en el ejercicio de sus competencias, como en su régimen patrimonial y de contratación, es compatible con su naturaleza de autoridad pública independiente, encargada de velar por la privacidad y la protección de los datos personales de todos los ciudadanos. Por otro lado, la reforma que experimentó en el año 2003 la Ley Orgánica de Protección de Datos mejoró notablemente el nivel de transparencia de la actuación de la Agencia, al exigir la publicación de todas sus resoluciones, preferentemente a través de medios informáticos o telemáticos utilizando la página web de la Agencia, lo que ha facilitado el conocimiento generalizado de los criterios de aplicación de la normativa, contribuyendo así al incremento de la seguridad jurídica.

Por ello, creo que la mejora de la AEPD no ha de centrarse tanto en el cambio de su régimen jurídico, como en la agilización de los procedimientos de protección de los datos personales y en la implementación de canales de información y contacto que faciliten la interacción con el ciudadano. Así, por ejemplo, tras la entrada en vigor del RGPD la Agencia ha de incrementar su colaboración con las empresas y con los autónomos, pues se convierten (los responsables y los encargados del tratamiento de datos) en sujetos directamente obligados al cumplimiento de una normativa nueva y compleja. Asimismo, de la Agencia depende que la figura del delegado de protección de datos sea una figura eficaz, por lo que deberá trabajar en una continua mejora de los cauces de comunicación, con la finalidad de que se articulen las medidas necesarias que garanticen la protección de los datos personales en el ámbito de la empresa. De igual manera, creo que también le corresponde el fomento de procedimientos de mediación para la resolución extrajudicial de reclamaciones, vinculados a códigos de conducta, que es una previsión del RGPD.

En relación con las amenazas que para la protección de los datos personales derivan del desarrollo tecnológico, la Unidad de Evaluación y Estudios Tecnológicos de la Agencia puede convertirse en una sede muy importante para estar al día de los avances y así poder adelantarse a la aparición de escenarios que pueden resultar un peligro directo para este derecho, todo ello en colaboración con organismos públicos y empresas privadas del ámbito tecnológico.

***

TITLE: *Academic survey about personal data protection*

ABSTRACT: *In this academic survey a group of Constitutional Law Professors answer some questions about personal data protection and its challenges in the digital society, the recognition of a fundamental right of data protection and its possibilities against the transnational threats, the way of recognition of that right in a national and supranational process, the role played by the legislators and the judges, and about the data protection agencies and its functions.*

RESUMEN: *En esta encuesta un grupo de profesores de derecho constitucional contestan un conjunto de preguntas sobre la protección de datos personales y los retos a los que se enfrenta actualmente, el reconocimiento*

de un derecho fundamental a la protección de datos y las posibilidades que tiene de garantizar la posición de los ciudadanos frente a las amenazas transnacionales, el camino seguido para construir dicho derecho tanto a nivel nacional como supranacional, el papel que han jugado el legislador y los jueces, así como sobre la existencia de las agencias de protección de datos y el lugar que ocupan.

KEY WORDS*: personal data protection, fundamental right to data protection, data protection law, data protection agencies.*

PALABRAS CLAVE*: protección de datos personales, derecho a la protección de datos, derecho de protección de datos, agencias de protección de datos.*