LAS TRANSFORMACIONES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Por el Académico de Número
Excmo. Sr. D. Pablo Lucas Murillo de la Cueva*

Sumario: 1. Los orígenes de un derecho fundamental.—2. El contenido del derecho fundamental a la protección de datos personales.—3. El cambio de perspectiva.—4. Los poderes públicos limitados y controlados.—5. El acceso masivo a los datos de las comunicaciones electrónicas.—6. El problema de la territorialidad de las regulaciones.—7. El caso de las transferencias de datos a los Estados Unidos de América.—8. La proyección política de los tratamientos de datos personales.—9. La responsabilidad individual.

El pasado mes de mayo celebramos en esta sala una reunión con profesores de Enseñanza Secundaria que participaban en una iniciativa de la Comunidad de Madrid dirigida a dar a conocer entre ellos a las Reales Academias. Al efectuar los preparativos, solicitamos a los responsables de la Consejería de Educación la relación de los que asistirían. La sorprendente respuesta recibida fue la de que no nos podían facilitar sus identidades porque no se lo permitía el derecho a la protección de datos de los interesados. Hubo que explicarles que a esta Real Academia le asiste el interés legítimo de conocer quiénes acceden a su sede, celebran una reunión en ella y visitan sus instalaciones y solo entonces accedieron a facilitarnos esa relación.

---

* Sesión del día 11 de octubre de 2022.

La anécdota refleja bien que este derecho sigue siendo un gran desconocido y que, mientras es ignorada su existencia por muchos, otros le atribuyen un alcance desmedido. Parece hallarse entre la nada y el todo. Por eso, me ha parecido adecuado volver sobre él.

1. LOS ORÍGENES DE UN DERECHO FUNDAMENTAL

Digo volver porque sobre este derecho versó el discurso de ingreso de nuestro compañero don Andrés Ollero Tassara, *De la protección de la intimidad al poder de control sobre los datos personales* el 18 de noviembre de 2008. Pero también es un nuevo regreso para mí porque ya en 1989[1] defendí su carácter de derecho fundamental, ínsito en el artículo 18.4 de la Constitución. Y, posteriormente, he podido examinar con regularidad determinados aspectos de su evolución y comentar sentencias y disposiciones que se han ocupado de él. Vuelvo, pues, una vez más porque a lo largo de los últimos años ha experimentado cambios importantes por obra de los legisladores o de los tribunales. Por ejemplo, poco antes del verano el Tribunal Constitucional dictó la sentencia núm. 89/2022, de 29 de junio, con una nueva aproximación al llamado derecho al olvido.

Este derecho a la protección de datos personales busca ofrecernos medios para defendernos de los perjuicios que nos puede deparar el uso incontrolado por terceros de la información que nos identifica, ya sea en el ámbito de nuestra vida privada, ya sea en la esfera de la actividad que desarrollamos de cara a los demás y no nos inquieta que vean y conozcan. La preocupación por establecer límites al acceso a los datos personales surgió, primero, frente al poder público –el temor al Gran Hermano orwelliano– pero con el tiempo y con los progresos constantes de la tecnología de la información y de las comunicaciones se ha extendido a los que podemos llamar poderes privados y, a menudo, los problemas vienen más de estos últimos que de aquél.

En España fue reconocido como derecho fundamental por la sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre[2]. Sentencia que recogió los planteamientos que en sede académica abogaban por tal reconocimiento y vino a coincidir temporalmente con la aprobación en la cumbre de jefes de Estado y de Gobierno de la Unión Europea de Niza, en los primeros días de diciembre de 2000, de la Carta de los Derechos Fundamentales que incluye al de protección de datos entre ellos como una categoría autónoma,

---

[1] Lucas Murillo de la Cueva, P., *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

[2] Acompañada de la núm. 290/2000, también de 30 de noviembre, sobre las competencias autonómicas en la materia, culminó una línea de jurisprudencia que arranca de la sentencia núm. 254/1993.

distinta del derecho a la intimidad o del derecho a vida privada. La Carta era entonces un documento político, sin efectos jurídicos, pero su importancia no podía desconocerse por su contenido y por quiénes la habían aprobado. También he llamado la atención sobre la circunstancia de que en el año 2000 el Tribunal Europeo de Derechos Humanos, en sus sentencias de 16 de febrero (*Amann contra Suiza)* y de 4 de mayo (*Rotaru contra Rumania)* declaró que el derecho a la vida privada reconocido en el artículo 8 del Convenio de Roma comprende el de la protección de datos de carácter personal.

Esta triple coincidencia[3] proyectó este derecho, al que se consideraba una manifestación de los de la llamada tercera generación, al máximo rango jurídico y dio un nuevo y más consistente fundamento a la legislación que se había ocupado hasta entonces de proteger los datos personales y a la jurisprudencia dictada a propósito de ella.

Hoy en día el derecho fundamental que en España tiene, según se ha dicho, su asiento en el artículo 18.4 de la Constitución, se encuentra reconocido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, la cual desde el Tratado de Lisboa de 13 de diciembre de 2007 forma parte de su Derecho originario y está regulado por el Reglamento (UE) 2016/679, del Parlamento y del Consejo, de 27 de abril de 2016. Y, en el ámbito del Consejo de Europa, su Protocolo 223, en fase de ratificación[4], ha puesto al día el Convenio núm. 108, de 28 de enero de 1981, sobre la protección de las personas frente al tratamiento automatizado de los datos personales[5] –que fue en su momento la principal referencia normativa en la materia– en términos semejantes a los del Reglamento de la Unión Europea.

Al punto en que nos encontramos se ha llegado al cabo de un amplio período en el que inicialmente no se consideró imprescindible una regulación específica entre otras razones porque no se vislumbraba la necesidad de reconocer un derecho fundamental distinto del que ya estaba presente en las Constituciones y en los documentos internacionales y protegía la intimidad o la vida privada. A pesar de que eran patentes los desarrollos tecnológicos que permitían acceder cada vez con mayor facilidad a información personal, elaborarla, conservarla y recuperarla con rapidez, a pesar de que nuestros constituyentes,

---

[3] A ella me he referido en «La aproximación judicial al derecho a la protección de datos personales», en *Protección de Datos y Cámaras Legislativas*. Parlamento Vasco, Vitoria, 2019, pp. 33 ss.

[4] Entrará en vigor cuando lo hayan ratificado todos los Estados parte o el 11 de octubre de 2023 si en esa fecha lo hubieren ratificado 38 Estados. En la actualidad son 19 los que lo han hecho. España lo ratificó el 28 de enero de 2021. Cfr.: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[5] El Convenio 108 fue ratificado por España por instrumento de 27 de enero de 1984 *(Boletín Oficial del Estado* del 15 de noviembre de 1985). En 2001 se aprobó el Protocolo Adicional núm. 181 para añadir a las exigencias relativas a la protección de datos la creación de autoridades independientes de garantía. España lo ratificó mediante instrumento de 20 de mayo de 2010 *(Boletín Oficial del Estado* del 20 de septiembre).

al igual que antes los constituyentes portugueses, percibieron los peligros de la automatización de la información personal, sin embargo en la mayoría de los Estados no se establecieron entonces disposiciones específicas para impedir que esas capacidades revirtieran en perjuicios para los individuos a quienes correspondían los datos tratados. Hay que reconocer que entonces la utilización de medios informáticos no tenía la extensión e intensidad que alcanzaría no mucho más tarde.

Esta circunstancia terminó influyendo también en España, pues tras el gran paso dado por la Constitución al encomendar al legislador limitar el uso de la informática para garantizar los derechos al honor y a la intimidad personal y familiar y el pleno ejercicio de sus derechos por los españoles, nada se hizo hasta 1992. Mejor dicho, lo único que se hizo fue incluir una disposición transitoria en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, según la cual sus prescripciones serían aplicables a las intromisiones ilegítimas derivadas del uso de la informática en esos derechos mientras no se promulgara la ley prevista en el artículo 18.4 de la Constitución. Precepto aquél que no tuvo aplicación práctica porque la regulación de esa Ley Orgánica, todavía en vigor, no responde a los problemas que supone el tratamiento de los datos personales.

Aunque ya en 1977 la República Federal de Alemania se había legislado al respecto y Francia lo hizo en 1978[6] y, a pesar de que el Convenio núm. 108 de 1981, del Consejo de Europa ofrecía las bases materiales del nuevo derecho, carecimos de regulación hasta finales de 1992, que es cuando se aprueba la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD)[7], vigente hasta que fue sustituida en 1999 por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), cuyo contenido era sustancialmente el mismo que el de la LORTAD salvo en algunos detalles[8].

Esa sustitución obedeció a la necesidad de adaptar la legislación española a la Directiva 95/46/CE[9]. Se puede llamar ya la atención sobre la doble aproximación de la Unión Europea al derecho que nos ocupa: se propone pro-

---

[6] Las primeras leyes se dictaron en el *land* de Hesse en 1972 y en Suecia en 1973. Se referían a los tratamientos realizados por las Administraciones públicas. Cfr. Lucas Murillo de la Cueva, P., *El derecho a la autodeterminación informativa*, cit. pp. 130 ss.

[7] Sobre la LORTAD, cfr. Lucas Murillo de la Cueva, P., *Informática y protección de datos personales. Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal,* Centro de Estudios Constitucionales, Madrid, 1993.

[8] Sobre la LOPD, cfr. Antonio Troncoso Reigada (director), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas-Thomson Reuters, Cizur Menor, 2010.

[9] La Unión Europea esperó hasta 1995 para dictar 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.

tegerlo pero también pretende asegurar la libre circulación de los datos personales. Libre circulación entre los Estados miembros y, además, fuera de la Unión siempre que tengan por destino países con un nivel de protección equivalente al europeo. Porque, y esta es otra observación que se debe hacer ya, la información personal se había convertido en un bien valiosísimo desde el punto de vista económico, valor que se ha ido incrementado de tal modo que se dice que es el oro negro del siglo XXI.

Bajo la Directiva 95/46/CE los distintos países miembros que carecían de ellas fueron aprobando las correspondientes leyes de protección de datos y los que, como España, disponían ya de ellas, las adaptaron y así la Unión Europea pasó a contar con una regulación, si no uniforme, porque las soluciones no eran idénticas, sí con un alto nivel de homogeneidad.

Ahora bien, con los años, de la mano del avance y el refinamiento vertiginosos de la tecnología, el tratamiento de datos personales se ha ido haciendo cada vez más sencillo y, también, más imprescindible en todos los niveles y los flujos de información de esta naturaleza han ido creciendo exponencialmente a la par que su trascendencia económica. Esa es la razón por la que se consideró necesario dar un paso más y superar a escala europea una situación en la que la falta de uniformidad de las legislaciones, pese a su sustancial proximidad, era fuente de problemas, sobre todo para los flujos transfronterizos de datos y para la seguridad jurídica de operadores y empresas que actúan en varios países y, por eso, se pusieron en marcha los trabajos que culminaron, tras varios años de intensos trabajos, en el Reglamento (UE) 2016/679.

Al mismo tiempo, la puesta al día por el Consejo de Europa del Convenio núm. 108 por el Protocolo 223 ha consistido en recoger una regulación sustancialmente igual a la del Reglamento (UE) 2016/679, si bien con una importante diferencia: el nuevo texto se centra en el derecho a la protección de datos y no menciona la libertad de circulación de los mismos. Naturalmente, el distinto enfoque no significa que no exista esta última ni que no pueda suponer un límite al derecho fundamental pero sí pone de manifiesto que este es lo principal. Habrá que ver si el Tribunal de Estrasburgo saca consecuencias de ello.

En España, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de los derechos digitales, ha sustituido a la LOPD. Dado que el Reglamento (UE) 2016/679 rige directamente en todos los Estados miembros de la Unión Europea y que contiene un ordenamiento sustancialmente completo, los legisladores de los Estados miembros de la Unión Europea y, por tanto, el español, han tenido que derogar sus anteriores leyes y dictar otras nuevas con aquellas determinaciones que el Reglamento (UE) 2016/679 expresamente les ha encargado y las que se han considerado necesarias para su mejor aplicación. Este es el sentido de la Ley Orgánica 3/2018, que también incorpora un catálogo de derechos digitales para llevar a espacios

a los que han migrado relaciones antes establecidas directa y personalmente la garantía ofrecida en el mundo analógico. Además del ordenamiento general que aportan el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, otras leyes contienen preceptos específicos sobre la protección de datos personales en ámbitos sectoriales señalados[10].

2. EL CONTENIDO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES

Conviene, antes de continuar, recordar que el derecho fundamental a la protección de datos de carácter personal se reconoce a las personas físicas, comprende todos los datos, de cualquier naturaleza, que permitan su identificación, tengan carácter íntimo o no. Supone la facultad de consentir o no el tratamiento automatizado de tales datos, exigir el respeto a las condiciones en que las leyes autoricen efectuarlo sin ese consentimiento –más rigurosas cuando tenga por objeto datos relativos a la ideología o creencias o a la afiliación política o sindical y a la salud, todos ellos considerados datos sensibles por su estrecha relación con otros derechos fundamentales– y de oponerse a que terceros pretendan llevarlo a cabo en virtud de un interés legítimo que pueda asistirles.

Además, comporta el derecho a conocer qué datos personales del titular disponen terceros, el de rectificarlos si son incorrectos o cancelarlos. Siempre desde la perspectiva del sujeto activo, del titular del derecho, hay que decir que entre las facultades que comprende este derecho fundamental se incluye, además, la de ser informado de la existencia de decisiones automatizadas, incluida la elaboración de perfiles, de la lógica aplicada, así como de la importancia y de las consecuencias del tratamiento para el interesado (artículo 15.1 h) del Reglamento (UE) 2016/679. Por su parte, el Protocolo 223 del Consejo de Europa incluye el derecho de las personas a obtener información del razonamiento subyacente al tratamiento de datos cuando se le apliquen los resultados de ese tratamiento (artículo 9).

Desde la perspectiva del sujeto pasivo, es decir de quien trata datos de otras personas, este derecho fundamental le obliga a contar con un título jurí-

---

[10] Es el caso de las recientes leyes orgánicas que se han ocupado de la protección de datos en la Administración de Justicia y en el proceso penal. Se trata de la Ley Orgánica 7/2015, de 1 de julio, por la que se modifica la Ley Orgánica del Poder Judicial, y de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Antes se establecieron preceptos al respecto, entre otras, en la Ley 58/2003, de 17 de diciembre, General Tributaria, y en la Ley Orgánica 2/2006, de 3 de mayo, de Educación. Y en el ámbito sanitario la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, introdujo prescripciones muy importantes.

dico –que puede ser el consentimiento informado y explícito del afectado, la previsión legal o la posesión por quien hace el tratamiento de un interés legítimo– que lo fundamente. Esa habilitación no es general ni incondicionada, ni permanente, sino referida a una finalidad lícita específica y su utilización ha de respetar los principios de calidad de los datos. Es decir, el tratamiento se deberá circunscribir a los que sean correctos, pertinentes, estén al día y resulten necesarios para perseguir esa finalidad. Por tanto, el error, el exceso, la pérdida de actualidad o de la imprescindible conexión con la finalidad para la que se recogieron los datos determina la improcedencia de proseguir su tratamiento.

Este derecho fundamental comprende, además, una dimensión institucional en la medida en que exige la creación de una autoridad independiente a la que se le confía una primera línea de defensa especializada del mismo, sin perjuicio de que jueguen también todas las garantías previstas por el ordenamiento jurídico para preservar los derechos. En España es la Agencia Española de Protección de Datos, creada en 1993[11], y en otros países existen organismos semejantes, bien monocráticos, bien colegiados y lo mismo sucede en la Unión Europea con el Comité Europeo de Protección de Datos previsto por el Reglamento (UE) 2016/679[12].

Junto a la tipificación en los códigos penales de específicos delitos que castigan las conductas más graves, se debe destacar el severo régimen sancionador que castiga principalmente con multas muy severas las infracciones al régimen jurídico que protege los datos de carácter general. El catálogo de infracciones y de las correspondientes sanciones se encuentra en el Reglamento (UE) 2016/679 (artículo 83). La potestad para aplicarlo reside en las mencionadas autoridades independientes.

En conjunto, vemos que este derecho fundamental, aunque de la forma tardía que he señalado, ha terminado siendo objeto diversas regulaciones hasta llegar a la actualmente vigente, cuya densidad y especialización son particular-

---

[11] Al amparo de la LORTAD, primero, y de la LOPD después se crearon Agencias de Protección de Datos en varias Comunidades Autónomas con competencia sobre los ficheros de titularidad pública autonómica o local. Fue el caso de la Agencia de la Comunidad de Madrid, creada por la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos por la Comunidad de Madrid. Realizó una importante labor pero fue suprimida el 1 de enero de 2013 como medida de reducción del gasto público por la Ley 8/2012, de 28 de diciembre, de medidas fiscales y administrativas, reintegrándose sus funciones a la Agencia Española de Protección de datos, según el artículo 61.2 de este texto legal. En Cataluña la Ley 5/2002, de 19 de abril, creó la Agencia Catalana de Protección de Datos y la Ley 32/2010, de 1 de octubre, la sustituyó por la Autoridad Catalana de Protección de Datos. En el País Vasco la Ley 2/2004, de 25 de febrero, de ficheros de datos de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, instituyó este ente. En Andalucía se han encomendado las tareas al Consejo de Protección de Datos y Transparencia de Andalucía por la Ley 1/2014, de 24 de junio.

[12] Bajo la Directiva 95/46/CE se creó el Supervisor Europeo de Protección de Datos conforme al Reglamento (CE) núm. 45/2001, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de datos.

mente acusadas. Si, además, tenemos en cuenta el creciente desplazamiento al llamado ciberespacio o, si se prefiere, al mundo virtual o digital, de cada vez más relaciones públicas y privadas, resulta clara la trascendencia presente y futura de este instrumento jurídico[13].

3. EL CAMBIO DE PERSPECTIVA

Una vez expuestos el origen y el desarrollo de este derecho y los aspectos principales de su contenido, conviene llamar la atención sobre las transformaciones principales que ha ido experimentando su ordenación jurídica y sobre la manera en que se han producido.

La primera que hay que señalar es la relativa al cambio de enfoque del propio sistema de protección. Seguramente por influencia de las primeras legislaciones, las adoptadas a principios de los años setenta del siglo pasado, la orientación adoptada por las leyes era la propia de la intervención administrativa. Se explica porque esas primeras leyes se dirigían principalmente a limitar y controlar el tratamiento de datos por las Administraciones Públicas. Así, las aprobadas en los años ochenta y noventa del siglo xx, una vez fijados los principios, en línea con el Convenio núm. 108 del Consejo de Europa, articularon un sistema que descansaba en la distinción entre los ficheros de titularidad pública y los ficheros de titularidad privada, exigiendo para los primeros una disposición general que los creara y para los segundos la comunicación previa de su creación y de sus elementos distintivos. Unos y otros debían ser inscritos en un Registro General de Protección de Datos y quedaban bajo la supervisión e inspección de la Agencia Española de Protección de Datos.

La Directiva 95/46/CE inició el cambio operado ya definitivamente por el Reglamento (UE) 2016/679. Ha supuesto poner el acento, no en los ficheros ni en su distinción en públicos y privados, sino en los tratamientos, en las operaciones sobre los datos personales, a fin de lograr que se ajusten a los principios de calidad y respeten los límites que impone el derecho fundamental de los afectados, ya se realicen por las Administraciones Públicas, ya los efectúen los operadores privados. Es el nuevo un enfoque esencialmente material y dinámico frente al predominantemente formal y estático anterior.

Han debido transcurrir más de veinte años para que se completara este cambio. Pensemos que en España la LOPD, vigente hasta que la desplazó la

---

[13] Para una visión completa del régimen jurídico del derecho a la protección de datos puede consultarse Antonio Troncoso Reigada (director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales* (2 vols.), Civitas-Thomson-Reuters, Cizur Menor, 2021.

entrada en vigor del Reglamento (UE) 2016/679, en mayo de 2018 y luego la derogó la Ley Orgánica 3/2018, descansaba sobre la diferenciación entre ficheros según su titularidad.

No ha sido ésta la única variación significativa. Frente a la opción primera consistente en confiar sobre todo a la acción administrativa la aplicación de los principios sustantivos de la protección de datos personales, la actual descansa más en la promoción de las condiciones adecuadas para que dichos principios sean respetados. Esto se consigue estableciendo un marco jurídico para el tratamiento de datos personales sin trabas previas pero exigiendo a quien pretenda llevarlo a cabo, además de un título jurídico que le legitime para ello y del respeto a los límites impuestos por el Reglamento y la adopción de medidas de seguridad de los datos, medidas preventivas de diversa naturaleza: desde la evaluación de impacto, el análisis de los riesgos y la consulta previa hasta la obligación de dotarse, cuando el tratamiento lo efectúen las Administraciones Públicas o sea a gran escala o verse sobre datos sensibles, de delegados de protección de datos.

Estos últimos deberán participar en todas las cuestiones relativas a la protección de datos personales y serán el punto de contacto de la autoridad de control. Es este un requerimiento organizativo importante. Igualmente, es importante la obligación impuesta a los responsables y encargados de los tratamientos de llevar un registro de actividades. Otra obligación relevante es la de notificar a la autoridad de control las violaciones de la seguridad de los datos y la de notificarla también a los afectados cuando haya un alto riesgo para sus derechos.

Por otro lado, el Reglamento incentiva los códigos de conducta y las buenas prácticas y otras actuaciones encaminadas a promover la protección de datos, sea desde el diseño de los aparatos y programas, sea desde la organización y funcionamiento de los operadores o hacerla valer por defecto. Es una solución pragmática especialmente adecuada para los tratamientos que se hacen fuera de las Administraciones Públicas.

Una ulterior modificación es la que ha supuesto el endurecimiento de las sanciones pecuniarias. El Reglamento (UE) 2016/679 ha incrementado de forma extraordinaria la cuantía de las multas, hasta 40 millones de euros las más elevadas o, si se trata de empresas, al 4% del volumen de negocio anual en el ejercicio anterior, si fuere superior. Es la contrapartida a la falta de imposición de controles previos y de la mayor confianza que pone en que quienes tratan datos personales lo van a hacer respetando el derecho fundamental.

La orientación seguida por el Reglamento responde, no solo a la búsqueda de la eficacia. También se explica porque la realidad ha puesto de manifiesto que no es del ámbito del poder público de donde proceden los principa-

les motivos de preocupación. Me refiero, obviamente, a los poderes públicos de los Estados democráticos. En ellos, el Estado de Derecho y el control político y judicial al que están sujetas las Administraciones dificultan –cuando no impiden– que estas incurran en excesos y, desde luego, corrigen los que se produzcan. En cambio, es mucho más difícil preservar el derecho fundamental en las innumerables relaciones privadas en que se producen tratamientos de datos personales por una multiplicidad de sujetos. Tanto los que tienen lugar a pequeña escala cuanto los que son a gran escala.

Sorprendentemente, con el paso del tiempo, los problemas principales en materia de protección de datos personales han venido, están viniendo, más que de los poderes públicos, de operadores privados. No es necesario pensar en las grandes empresas tecnológicas radicadas fuera de la Unión Europea, que también, sino en cualquiera que capte información personal por cualquier medio, la elabore y la transmita a terceros. Es sorprendente el grado de conocimiento que es posible alcanzar, no ya de grupos de personas, sino de individuos concretos al objeto de clasificarles, atribuirles preferencias y dirigir hacia ellos campañas singulares o de adoptar decisiones que les afectan.

La navegación por internet es un buen ejemplo del reguero de datos que vamos dejando tanto para el buscador que utilicemos cuanto para los titulares de las páginas o sitios que visitemos. Normalmente, no nos dirán qué es lo que retienen de nosotros o, a lo sumo, pedirán nuestro consentimiento para usar *cookies* y nos remitirán, si queremos saber más, a prolijos documentos escritos en una jerga de difícil comprensión incluso para quienes cuentan con formación. Si seguimos adelante en nuestra navegación comprobaremos enseguida que en esas páginas, aunque sean extranjeras, comenzará a aparecer publicidad de establecimientos, servicios o productos por los que nos hemos interesado poco antes aunque no tengan que ver con la información que buscamos. Es un pequeño detalle que muestra que se ha registrado qué es lo que buscamos.

Es verdad que nos suelen explicar que retienen nuestros datos personales para atendernos mejor pero no suelen decir, qué hacen después con ellos. El problema, sin embargo, no es el de que quien gestiona un determinado sitio quiera saber qué nos interesa para darnos un mejor servicio, sino que retiene esa información que nos concierne y puede trasladarla a otros, abriendo la posibilidad de que se integre con la que procede de fuentes diferentes y, así, se incremente el caudal de datos con los que se nos ordena y acabe sirviendo para que se adopten decisiones sobre nosotros, ya sea a partir de perfiles, ya sea a partir de una determinada circunstancia a la que se nos asocie, con independencia de que sea cierta o no y sin que podamos defendernos o debamos tomar la iniciativa de las reclamaciones y denuncias.

4. LOS PODERES PÚBLICOS LIMITADOS Y CONTROLADOS

Decía que la preocupación en lo que concierne a la protección de datos personales no debe dirigirse tanto hacia el poder como se temió inicialmente, sino hacia la sociedad. Mejor dicho en dirección a los sujetos privados que tratan esos datos. Debo precisar esta afirmación.

Tanto en España como en otros países democráticos existe la inquietud por la intromisión de las fuerzas y cuerpos de seguridad y por los servicios de inteligencia en la vida privada mediante la interceptación de las comunicaciones de cualquier clase, el recurso a la videovigilancia o cualquier otro medio que permita dicha injerencia. A este respecto, he de indicar que por comunicación, cuando tiene lugar por medios electrónicos, se entiende no solo el contenido –la conversación, el texto, las imágenes o signos o símbolos– que se transmite, sino también los metadatos. Es decir, aquellos elementos externos, relativos a la localización de los partícipes en la comunicación, a la identificación de los números telefónicos o protocolos de internet (IP) y de los medios de que se sirven y a la fecha y hora en que tiene lugar. Además, conviene señalar que las entidades operadoras de los servicios de comunicaciones electrónicas están obligadas a retener los datos relativos al tráfico de las mismas durante un período determinado que en España, conforme a la Ley 25/2007, de 18 de octubre de 2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas, es de un año.

No es cuestión menor porque el artículo 18.3 de la Constitución nos reconoce el derecho al secreto de las comunicaciones, salvo resolución judicial. Ahora bien, en lo que se refiere a la prevención e investigación de los delitos, contamos con una regulación de estas cuestiones en la Ley de Enjuiciamiento Criminal suficientemente garantista pues solamente el juez penal competente puede autorizar medidas de esa naturaleza en el curso de la instrucción procesal por delitos si es que la policía le presenta una justificación suficiente. Y, en el caso del Centro Nacional de Inteligencia, si para el cumplimiento de sus funciones necesitare acceder a las comunicaciones de determinada persona, deberá obtener antes la autorización motivada del magistrado del Tribunal Supremo competente al efecto, al que habrá debido justificar esa necesidad en términos concretos, conforme a la Ley Orgánica 2/2002, de 6 de mayo, y a la Ley 11/2002, de 6 de mayo. Y la Ley 25/2007 antes mencionada subordina a la autorización judicial previa el acceso a los metadatos siempre que se trate de la investigación de delitos graves o de las funciones del Centro Nacional de Inteligencia.

Por su parte, en materia de videovigilancia la Ley Orgánica 4/1997, de 4 de agosto, exige la autorización de una comisión específica presidida por el Presidente del Tribunal Superior de Justicia correspondiente para que las Fuerzas y Cuerpos de Seguridad utilicen videocámaras en lugares públicos y

prohíbe que capten imágenes del interior de los domicilios o establecimientos sin consentimiento de los afectados o autorización judicial.

No tengo que decir que los jueces se toman en serio esta responsabilidad.

5. EL ACCESO MASIVO A LOS DATOS DE LAS COMUNICACIONES ELECTRÓNICAS

Por lo que hace al acceso masivo a las comunicaciones electrónicas por los servicios de inteligencia conviene señalar que no lo han rechazado ni el Tribunal Europeo de Derechos Humanos ni el Tribunal de Justicia de la Unión Europea aunque, claro está, ambos exigen que se produzca en un contexto caracterizado por garantías suficientes que impidan abusos o excesos.

Así, el primero en la sentencia de su Gran Sala de 25 de mayo de 2021 (caso *Big Brother Watch and others versus United Kingdom*), relativa a la queja de diversas organizaciones de defensa de los derechos humanos y de la democracia y de periodistas y abogados, tras las revelaciones de Edward Snowden sobre los programas de vigilancia electrónica operados por los servicios de inteligencia de Estados Unidos y del Reino Unido. Estos recurrentes plantearon al Tribunal de Estrasburgo su convicción de que, por la naturaleza de sus actividades era probable que sus comunicaciones hubieran sido interceptadas por los servicios de inteligencia del Reino Unido o que estos hubieran tenido acceso a ellas a través de interceptaciones practicadas por gobiernos extranjeros y/o obtenidas por las autoridades del Reino Unido de los proveedores de servicios de comunicaciones. La Gran Sala ha fallado que, tanto el acceso a las comunicaciones mediante rastreos generales cuanto la comunicación de los datos así obtenidos por los servicios de inteligencia, han supuesto la vulneración del artículo 8 Convenio de Roma[14]. Ahora bien, ha fundamentado ese pronunciamiento en la falta de las debidas garantías. Su sentencia, pese a reconocer que el Reino Unido no abusó de sus facultades, explica que la infracción viene de la insuficiente calidad de la ley que las prevé[15].

Es más, reconoce expresamente que el acceso masivo a las comunicaciones electrónicas (*bulk interception*) es de vital importancia para la seguridad

---

[14] También apreció la vulneración del artículo 10 del Convenio, que reconoce la libertad de expresión e información, porque se vieron afectadas las comunicaciones de periodistas.

[15] Principalmente, por no estar prevista una supervisión independiente, no exigir la inclusión de los selectores a utilizar en la solicitud de autorización y no contemplar el uso de los relacionados con un determinado individuo a una previa autorización interna.

de los Estados democráticos, tal como ha reconocido también la Comisión de Venecia[16]. El panorama que describe para llegar a esa conclusión es este:

> «While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and the sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyber-attacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there».

De ahí que el Tribunal de Estrasburgo considere que:

> «Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate».

Para ello, exige que la Ley que contemple dicha interceptación contenga con absoluta claridad estas salvaguardias mínimas: (i) identifique la naturaleza de los delitos que pueden justificar la interceptación; (ii) defina las categorías de personas cuyas comunicaciones pueden ser interceptadas; (iii) fije un límite temporal a la interceptación; (iv) establezca el procedimiento a seguir para examinar, usar y almacenar los datos obtenidos; (v) defina las precauciones a tomar en la comunicación de los datos a terceros; y (vi) las circunstancias en las que esos datos pueden ser borrados o destruidos. Además, deberá prever (vii) un régimen de supervisión de la aplicación de las medidas secretas de vigilancia y mecanismos de notificación y de recurso (viii).

En cambio, no ha considerado contrario al Convenio de Roma la recepción por el Reino Unido de materiales informativos facilitados por servicios de inteligencia extranjeros ya que hay un procedimiento establecido al efecto.

Por lo que hace al Tribunal de Justicia de la Unión Europea hay que recordar que en 2014 declaró inválida la directiva de retención de datos[17], no

---

[16] Es importante su informe sobre *Democratic Oversight of the Security Services and of Signals Intelligence Agencies*, accesible en www.venice.coe.int/documents.

[17] Sentencia de 8 de abril de 2014 (caso *Digital Rights Ireland)*. Conviene señalar que la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, sobre la conservación de datos generados o tratados en

porque no considerara justificada la exigencia de que se retuvieran temporalmente, sino porque las garantías previstas no eran suficientes: principalmente, la indeterminación de los afectados, la amplitud del período de conservación y la falta de la garantía judicial. Años después, en la sentencia de 6 de octubre de 2020 (asunto C-623/17, caso *Privacy International*), dijo que una legislación nacional que requiera a los proveedores de servicios de comunicaciones electrónicas transmitir de manera generalizada e indiferenciada datos de tráfico y de localización a agencias de seguridad e inteligencia a fin de proteger la seguridad nacional, excede los límites de lo que es estrictamente necesario y no podría ser considerado justificado en los términos de la Directiva interpretada a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, esencialmente porque afecta a todos los usuarios de los servicios de comunicación. Es decir, a personas respecto de las que ningún indicio hay de que lleven a cabo actividades contrarias a la seguridad nacional.

En esta línea la sentencia de la Gran Sala de 6 de octubre. de 2020 (asuntos C-511/18, C-512/18 y C-520/18, caso *La Quadrature du Net and others*)[18] ha dicho que el Derecho de la Unión y, en particular, el artículo 23.1 del Reglamento (UE)2016/679, interpretado a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales, se opone a la imposición a los proveedores de servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la obligación de conservar de manera generalizada e indiferenciada los datos de carácter personal correspondientes a esos servicios.

No obstante, esa misma sentencia ha afirmado que el Derecho de la Unión Europea no se opone a que el Estado miembro que se enfrente a una amenaza grave a su seguridad nacional real y actual o previsible, requiera a los proveedores de servicios de comunicaciones electrónicas retener de forma general e indiscriminada los datos de tráfico y localización durante el periodo de tiempo limitado que sea estrictamente necesario pero que podría ser ampliado si la amenaza persistiera. Tampoco se opone, dice esa sentencia, a que, a fin de combatir la criminalidad grave y de prevenir amenazas graves a la seguridad nacional, los Estados miembros exijan –por el tiempo limitado estrictamente necesario– la retención de datos de tráfico y localización en virtud de factores objetivos y no discriminatorios respecto de las categorías de personas concernidas o utilizar criterios geográficos o de direcciones IP asignadas a la fuente de una conexión de internet. Y no impide que los Estados obliguen a retener de manera general e indiscriminada los datos relativos a la identidad civil de los

---

relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE, declarada inválida por esta sentencia es la que fue transpuesta por nuestra Ley 25/2007 en vigor. La sentencia de 21 de diciembre de 2016 (asunto C-203/15 y C-698/15, caso *Tele 2 Sverige y Watso*n y otros) sigue la misma línea.

[18] Su texto fue modificado por el auto de 16 de noviembre de 2020.

usuarios de medios electrónicos de comunicación sin sujeción a específicos límites temporales. Ahora bien, han de existir normas claras y precisas que garanticen que la conservación de datos está supeditada al respeto de las condiciones materiales y procesales y a que las personas dispongan de garantías efectivas contra los riesgos de abuso.

Además, esta sentencia explica que el Derecho de la Unión Europea no se opone a que la normativa nacional obligue a los proveedores de servicios de comunicaciones electrónicas a recurrir al análisis automatizado y a la recopilación en tiempo real de los datos de tráfico y localización. Ahora bien, ha de ser un análisis limitado a supuestos de amenaza grave, real y actual a la seguridad nacional y ha de ser objeto de control efectivo de la concurrencia de esa situación por la autoridad judicial o por una autoridad independiente cuya decisión sea vinculante. Y la recopilación en tiempo real deberá limitarse a personas de las que se sospeche fundadamente que está implicadas en actividades terroristas, apreciación sometida al mismo control anterior.

Por tanto, el punto de llegada no se aleja del que marca la sentencia del Tribunal de Estrasburgo antes reseñada.

6. EL PROBLEMA DE LA TERRITORIALIDAD DE LAS REGULACIONES

Si desde la perspectiva específica anterior pasamos a una más amplia, la que ofrece la realidad de un flujo constante de información personal dentro y fuera de las fronteras, nos encontramos con el problema de que las legislaciones que protegen los datos personales rigen en el territorio de los Estados o de las Uniones de Estados que las dictan pero, en principio, no llegan más allá. Y, sin embargo, internet y las redes de comunicaciones electrónicas tienen una proyección universal por lo que es fácil que quien se lo proponga evite las restricciones locales operando desde lugares en los que no existen límites o son menos exigentes que en otros. La consecuencia es que resulta a menudo difícil y en ocasiones imposible defender este derecho fundamental de tratamientos realizados allí donde no llega la vigencia de los preceptos que buscan preservarlo.

Ciertamente, el remedio a los problemas que crean esos huecos, esos vacíos de legalidad o los regímenes más comprensivos o tolerantes con quienes tratan información personal sería el de contar con una regulación universalmente válida que no existe ni es previsible que exista en tiempos razonables si es que alguna vez se llegaren a dar las condiciones para establecerla. Por eso, es menester hacer uso de los instrumentos jurídicos disponibles para atraer a las regulaciones más exigentes a los operadores con domicilio exterior. Es lo que hizo el Tribunal de Justicia de la Unión Europea en la sentencia *Goo-*

gle v. Spain de 2014 a partir de la Directiva 95/46/CE y después ha establecido el Reglamento (UE) 2016/679 para someter al Derecho de la Unión a las grandes operadoras tecnológicas asentadas principalmente en los Estados Unidos. Dicho de manera sencilla, quienes cuentan con establecimientos o captan publicidad y obtienen ingresos por ella en el seno de la Unión Europea están sometidos a sus reglas en la materia.

Es, desde luego, un progreso pero con sus limitaciones, tal como se ha visto respecto del derecho al olvido, reconocido judicialmente a partir de la sentencia del caso *Google versus Spain* y plasmado en el Reglamento (UE) 2016/679[19]. Este derecho consiste en que, en las búsquedas por el nombre de una persona, los motores de búsqueda deben retirar de los resultados que ofrecen aquellos que hayan perdido actualidad. El Tribunal de Luxemburgo entendió que, exigiendo la Directiva 95/46/CE que los datos personales fueran actuales y adecuados a la finalidad para la que se recogieron, una vez perdidas esas cualidades por el transcurso del tiempo –se trataba de una información del periódico *La Vanguardia* de doce años antes sobre el anuncio de una subasta de inmuebles por deudas con la Seguridad Social en el que mencionaba el nombre de don Mario Costeja González– debía ser eliminada de entre los resultados por perjudicar al afectado una información desactualizada sobre él. Frente al derecho del público a conocer, el Tribunal de Justicia entendió que debía prevalecer, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales, el del Sr. Costeja González a la protección de su vida privada y de sus datos personales[20].

El reconocimiento de este derecho obligó a *Google* a poner en marcha un procedimiento para resolver las reclamaciones de quienes lo esgrimían y quienes no las vieron satisfechas acudieron a la Agencia Española de Protección de Datos –al igual que en otros paises los afectados se dirigieron a las respectivas autoridades de control– que, en general, acogió su pretensión y, dicho también en general, los tribunales confirmaron sus decisiones. El caso es que al llegar al momento de adoptar las medidas necesarias para satisfacer ese derecho al olvido *Google* optó por hacerlo efectivo únicamente en los accesos efectuados desde España o a lo sumo desde la Unión Europea,

---

[19] Sobre el derecho al olvido, véase Rallo Lombarte, A., *El derecho al olvido en Internet. Google versus Spain*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014; Simón Castellanos, P., *El régimen constitucional del derecho al olvido*, Tirant lo Blanch, Valencia, 2012. También, Jiménez-Castellanos Ballesteros, I., *El derecho al olvido digital del pasado penal*, Tirant lo Blanch, Valencia, 2021.

[20] Conviene precisar que este derecho al olvido no supone una suerte de censura ni implica la destrucción de la información afectada. Esta permanecerá allá donde se encuentre y se podrá acceder a ella sin más limitaciones que las propias del acceso a los registros, archivos, hemerotecas o bibliotecas en que se halle.

no en el resto del mundo. Tal respuesta fue considerada correcta por el Tribunal de Justicia[21].

No me parece una solución satisfactoria porque, si no se deben ofrecer los datos porque ya no tienen la exigida calidad, esa circunstancia invalida el tratamiento dondequiera que se realice. Además, si se trata de proteger la información personal, la protección debe ser efectiva y no lo es si se puede superar la prohibición efectuando las búsquedas desde servidores radicados en países externos a la Unión Europea, cosa que se puede lograr. El Tribunal Constitucional, dejó abierta esta cuestión suscitada en el debate resuelto por su sentencia núm. 89/2022.

7. EL CASO DE LAS TRANSFERENCIAS DE DATOS PERSONALES A LOS ESTADOS UNIDOS DE AMÉRICA

Es significativo que en los Estados Unidos, país que está a la cabeza del desarrollo tecnológico y donde tienen su sede y su domicilio las principales empresas tecnológicas del mundo, no exista una regulación federal del derecho a la protección de datos personales. Por eso, desde el momento en que la Unión Europea exige para autorizar las transferencias de información personal a países externos a ella que cuenten con un nivel de protección equivalente, ha sido necesario determinar si esa condición se da en los Estados Unidos. Y sucede que, por dos veces, el Tribunal de Justicia nos ha dicho que no.

En efecto, todavía bajo la Directiva 95/46/CE se buscó la fórmula mediante la cual se asegurara que las, por otra parte, imprescindibles transmisiones de datos a este país, se produjeran dentro de un marco jurídico que brindará seguridad a la propia información y a las empresas que realizaran las transferencias. La solución fue establecer un conjunto de acuerdos y prácticas, basadas principalmente en compromisos asumidos por la parte estadounidense, de respetar los principios de la Directiva. Todos ellos se plasmaron en una decisión de la Comisión Europea[22] que recogía los términos pactados a los cuales se les dio el nombre de *Safe Harbour* o Puerto Seguro, expresión con la que se quería significar el cumplimiento de la exigencia europea. Sin embargo, el Tribunal de Luxemburgo, en sentencia de 6 de octubre de 2015 (asunto C-362/14) declaró inválida la decisión. La razón principal fue que las

---

[21] Sentencia de 24 de septiembre de 2019 (asunto C-507/17). Sobre ella, véase Torralba, E., «Reflexiones sobre el alcance territorial del derecho al olvido», en *Cuadernos de Derecho Transnacional*, núm. 2/2021, pp. 575 ss., en especial 582 ss.

[22] Era la Decisión de la Comisión Europea 2000/520/CE, de 26 de julio de 2000.

autoridades públicas –entre ellas los servicios de inteligencia y seguridad– de los Estados Unidos disponían de acceso irrestricto a toda la información transferida sin que mediaran controles y limitaciones efectivas a esa potestad. La lectura de la sentencia revela bien a las claras esa injerencia.

Fue preciso, en consecuencia, encontrar un remedio que permitiera establecer un marco jurídico con el grado de protección de los datos equivalente al europeo. Y, tras las negociaciones consiguientes y mediando compromisos al más alto nivel de las autoridades estadounidenses, se fraguó otro acuerdo cuya denominación de conjunto es tan expresiva o más que la anterior: el *Safe Harbour* fue sustituido por el *Privacy Shield* o Escudo de la Privacidad[23]. Sin embargo, la decisión de la Comisión Europea que lo aprobó fue también declarada inválida por el Tribunal de Justicia en su sentencia de 16 de julio de 2020 (asunto C-311/18) por razones sustancialmente semejantes a las esgrimidas por la sentencia anterior. De manera que actualmente, mientras se fragua otra solución, no existe ese marco general y en cada caso quienes transfieren información personal a los Estados Unidos han de buscar en la contraparte garantías y cautelas que aseguren posibles responsabilidades y apoyarse en los títulos básicos de legitimación de los tratamientos que contempla el artículo 49 del Reglamento (UE) 2016/679.

No es necesario decir que en tanto se logre el necesario acuerdo, la realidad, en este caso la correspondiente al peso político, económico y de seguridad de los Estados Unidos de América tiende a imponerse sobre el cumplimiento estricto de la normativa europea. No obstante, en los supuestos en los que haya afectados que se vean perjudicados por un flujo de información personal que no esté sujeto a la protección exigida por el Reglamento (UE) 2016/679, tendrán derecho a ser resarcidos por esa sola circunstancia, al margen de las restantes responsabilidades que puedan hacer valer.

Así, pues, al igual que en otros ámbitos, la limitación territorial de la vigencia de las disposiciones normativas se traduce a su vez en la limitación de la protección buscada cuando se trata de actuaciones que se proyectan más allá de las fronteras. No obstante, la propia globalización de las relaciones sociales y económicas hace que en buena parte de los casos se den los puntos de contacto, las conexiones suficientes, para imponer a operadores externos el respeto al Derecho de la Unión Europea también en este campo.

---

[23] Decisión de Ejecución de la Comisión Europea 2016/1250/CE, de 12 de julio de 2016.

8. LA PROYECCIÓN POLÍTICA DE LOS TRATAMIENTOS DE DATOS PERSONALES

No solo es la seguridad de los Estados, ni la actividad económica la que explica la demanda de información personal. También la competencia por el poder político impulsa a los partidos, a las coaliciones y a otros actores interesados en influir en los procesos electorales o referendarios a hacerse con los datos a través de los cuales pueden deducir las preferencias de los ciudadanos a cuyo voto aspiran. De ese modo, pueden dirigir a cada sector de la opinión los mensajes que consideren útiles a sus fines: bien sea para movilizar a los proclives a sus planteamientos, bien sea para desmovilizar a los que no lo sean.

El caso de *Cambridge Analytica y* la utilización de datos personales obtenidos de la red social *Facebook* y la incidencia que pudo tener en las elecciones presidenciales de Estados Unidos de 2016 y en el referéndum del *Brexit* de ese mismo año es buena muestra de lo que puede significar el uso incontrolado de información personal en la contienda política. En el mismo sentido apunta la injerencia de Estados extranjeros en elecciones y referendos mediante la intoxicación de la opinión con noticias falsas, si bien en este caso no necesitan disponer de datos personales ya que les basta con inundar las redes con ellas, normalmente desde una multiplicidad de robots cubiertos por identidades falsas.

Nuestra experiencia no es ajena a estos peligros. Así lo indica el episodio surgido con la modificación de la Ley Orgánica del Régimen Electoral General, ni más ni menos que por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. La novedad consistió en añadir a aquella, a la LOREG, el artículo 58 bis, sobre la utilización de medios tecnológicos y datos personales en las actividades electorales. En particular, autorizaba a los partidos a recopilar en el marco electoral los datos personales relativos a las opiniones políticas de los ciudadanos siempre que en esa operación se contara con las garantías adecuadas.

La sentencia del Tribunal Constitucional 76/2019 declaró inconstitucional esa previsión por ser contraria al derecho a la protección de datos y a la libertad ideológica, así como a la seguridad jurídica. Estimó, en efecto, el recurso de inconstitucionalidad del Defensor del Pueblo esencialmente porque el legislador no había identificado las garantías a cuyo respeto se condicionaba la habilitación a los partidos para tratar datos relativos a las opiniones políticas. Hay que recordar que son de los que el legislador europeo y el español han calificado de sensibles y les han dado una protección reforzada por pertenecer al núcleo del derecho a la protección de datos personales y por su estrecha relación con otros derechos fundamentales.

9. LA RESPONSABILIDAD INDIVIDUAL

Según destacó hace dos siglos Benjamin Constant, en su célebre comparación entre la libertad de los antiguos y la libertad de los modernos[24], a diferencia de aquellos, que situaban esa libertad en su participación en el foro público, la de estos se orienta a preservar espacios de autonomía que les permitan excluir la injerencia de terceros en su ámbito. Y, ciertamente, esa preocupación explica el reconocimiento en el siglo pasado del derecho fundamental a la vida privada por el artículo 8 del Convenio de Roma y, más tarde, por nuestra Constitución del derecho a la intimidad al igual que ha sido reconocido el derecho a la *privacy*[25] por la jurisprudencia de diversos países y, hoy en día, la Carta de los Derechos Fundamentales de la Unión Europea reconoce, además del derecho a la protección de datos (artículo 8), el derecho a la vida privada (artículo 7).

Creo que, en general, existe o ha existido una amplia conciencia del derecho a la intimidad y que, también, dicho en general, nos preocupamos por reservarla a las personas próximas con las que compartimos vida, afectos e inquietudes y reaccionamos para defender esa esfera cuando sufrimos intromisiones ilegítimas en ella. No obstante, creo que esa tendencia quiebra en gran medida cuando de la comunicación a través de las redes sociales se trata. Una gran parte de quienes se mueven en ellas no tienen inconveniente en manifestar ideas de todo tipo y de mostrarse a sí mismos de las maneras más variadas. Por otro lado, ningún obstáculo se ve habitualmente –lo decía antes– en navegar por la red, ni en utilizar las aplicaciones más variadas a pesar del reguero de información personal que se va diseminando por todos los sitios visitados.

Contrasta, desde luego esa falta de preocupación y la desinhibición apreciable en innumerables personas que no deben ser conscientes de que nada de lo que entra en la red desparece. No parecen saber que en la sociedad de la era digital no hay olvido sino memoria, ni que, a lo sumo, como se ha visto, se puede lograr que no se recupere la información personal accesible cuando se solicite de un determinado modo, con el nombre y apellidos del afectado.

Y, sin embargo, la disponibilidad ilimitada e incontrolada por terceros de datos personales puede ser fuente de serios perjuicios directos para los afec-

---

[24] Constant, B., «De la libertad de los antiguos, comparada con la de los modernos», en *Escritos políticos*. Estudio preliminar, traducción y notas de María Luisa Sánchez Mejía. Centro de Estudios Constitucionales, Madrid, 1989, pp. 257 ss.

[25] Con arraigo antiguo en el *common law* según explicaron en su día Warren, S. D., y Brandeis, S. D., en su archicitado artículo «The right to privacy», *Harvard Law Review*. Vol. IV, 15 de diciembre de 1890, núm. 5. En la edición a cargo de Benigno Pendás y Pilar Baselga, *El derecho a la intimidad*, Civitas, Madrid, 1995, se ofrece traducido al español.

tados. De ahí que sea imprescindible insistir en la educación para la sociedad digital porque, por muy lograda que sea la legislación sobre la protección de los datos personales, de poco servirá si los titulares de este derecho fundamental desconocen que les asiste y, sobre todo, no observan en su acceso y permanencia en las redes ni, en general, en la navegación que hacen a través de ellas la elemental prudencia[26]. Es algo parecido a la educación vial: hay que enseñar y es preciso aprender a circular por los nuevos senderos virtuales que ha abierto la tecnología.

Solamente con esa educación con ese conocimiento será posible hacer valer este derecho. Como ocurre con todos, en la medida en que inciden en los de los demás, muy a menudo será necesario luchar por él. La lucha por el Derecho es una constante en la experiencia jurídica[27], es consustancial a la convivencia y no resulta una excepción el que me ha ocupado esta tarde.

---

[26] Sobre los problemas para la protección de datos en el mundo virtual de las redes sociales, véanse los trabajos recogidos en Artemi Rallo Lombarte y Ricard Martínez Martínez (coordinadores), *Derecho y redes sociales*, Civitas-Thomson Reuters, Cizur Menor, 2010.

[27] Rudolf Ihering lo puso de manifiesto en su obra clásica *La lucha por el Derecho* (traducción de Adolfo Posada, prólogo de Leopoldo Alas), Doncel, Madrid, 1976.