El nacimiento y la evolución del derecho a la protección de datos

PID_00246864

Luis Javier Mieres
Mònica Vilasau

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

1. La necesidad de protección de la vida privada frente a la tecnología: del derecho a la intimidad al derecho de protección de datos

Luis Javier Mieres

En el origen del reconocimiento de un derecho siempre existe la percepción de la necesidad de proteger un ámbito especialmente amenazado de la libertad humana. Dicho de otro modo, los derechos son la respuesta jurídica a las distintas amenazas para la dignidad y la libertad de las personas que se han ido identificando a la largo de la historia.

En este sentido, el progreso tecnológico está en la base del reconocimiento del derecho a la vida privada. Los riesgos que puede generar una sociedad tecnológicamente avanzada han determinado la necesidad de proteger la vida privada frente a las intromisiones que por cualquier medio pueden realizarse sobre los espacios o ámbitos en los que las personas desarrollan su esfera personal. Los avances tecnológicos permiten tener acceso, adquirir conocimiento, difundir y almacenar informaciones y datos sobre la vida de las personas que antes, en un mundo no tecnificado, resultaban naturalmente inaccesibles a los terceros.

Esta vinculación entre el derecho a la vida privada y el avance de la tecnología se puso ya de manifiesto en el famoso artículo «The Right to Privacy», que los juristas norteamericanos Samuel Warren y Louis Brandeis publicaron en la *Harvard Law Review* en 1890. En ese artículo los autores proponían el reconocimiento de un nuevo derecho fundado en el *common law* para proteger la dignidad personal como respuesta a los cambios propiciados por la expansión del uso de las nuevas tecnologías de la época: «Las instantáneas fotográficas y las empresas periodísticas –se lamentaban los autores– han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: "lo que se susurre en la intimidad, será proclamado a los cuatro vientos"». Warren y Brandeis sostenían que el reconocimiento del derecho a la *privacy* era el medio de garantizar lo que, usando la terminología de un jurista de la época, Thomas Cooley, podía denominarse «el derecho a no ser molestado» («*the right to be let alone*»), esto es, el derecho a decidir sobre el grado de exposición de su persona o de los hechos de su vida que el individuo está dispuesto a consentir.

Referencia bibliográfica

S. D. Warren; L. D. Brandeis (1890). «The Right to Privacy». *Harvard Law Review* (vol. 4, págs. 193-220). (Hay traducción española de Benigno Pendás y Pilar Baselga: *El derecho a la intimidad*. Madrid: Civitas, 1995).

La formulación académica del derecho a la privacidad tuvo inmediatamente eco en la jurisprudencia de los tribunales. En distintas sentencias a lo largo de los años siguientes se reconoció este derecho para estimar las pretensiones formuladas por los demandantes frente a periódicos, productoras de cine, agencias publicitarias, etc.

En otro famoso artículo publicado en la *California Law Review* en 1960, el profesor William Prosser analizó la jurisprudencia producida hasta entonces sobre la *privacy* y distinguió cuatro supuestos típicos de lesión de este derecho:

- La intrusión en la vida privada de una persona, esto es, la irrupción o entrada ilegal en un espacio o ámbito reservado frente a los demás.
- La revelación o divulgación de hechos relativos a la vida privada o íntima, cuando no exista un interés público en su conocimiento.
- La publicidad sobre una persona que distorsione o tergiverse la imagen de ella ante la sociedad; esto se refiere a la publicación de hechos sobre una persona descontextualizados o desfasados que proyecten sobre el público una imagen o visión de la persona que no se corresponda con la realidad.
- La apropiación con ánimo de lucro de la imagen de una persona, es decir, la captación y difusión de la imagen de alguien sin su consentimiento y con fines, básicamente, publicitarios.

Referencia bibliográfica

W. L. Prosser (1960). «Privacy». *California Law Review* (vol. 48, págs. 383-423).

De los cuatro casos típicos descritos por Prosser, los dos primeros se correspondían propiamente con la protección de la intimidad o vida privada, mientras que el tercero tenía más que ver con la protección del honor o la reputación social, y el cuarto con la protección de la propia imagen. En todo caso, el mérito del autor fue señalar los distintos contextos en los que la *privacy* podía ser lesionada, aunque en ninguno de los casos se ponía de manifiesto el potencial lesivo que podía tener el tratamiento automatizado de los datos personales en poder de los poderes públicos o de los actores privados.

Esa reflexión se inició en la década de los setenta y dio lugar a una visión de la *privacy* distinta de la tradicional. La visión del derecho a la vida privada como un derecho a ser dejado en paz, es decir, a no sufrir intrusiones o intromisiones por parte de terceros, suponía concebir el derecho como un derecho negativo del que se derivaban para los terceros un deber de abstención, de no hacer, consistente en no interferir o perturbar la vida privada de las personas.

En cambio, en el contexto del tratamiento de datos personales mediante la informática lo relevante era reivindicar el papel del individuo como «dueño» de sus datos y, por tanto, afirmar su poder de control sobre estos. Controlar el uso y destino de los datos personales de terceros implica para los sujetos obligados por el derecho la realización de determinadas acciones para hacer posible su ejercicio: solicitar su consentimiento para recoger y tratar los datos, informar sobre la finalidad del tratamiento de esos datos, cancelar o rectificar aquellos datos que el sujeto considera incorrectos o inexactos. De este modo, la protección de la dignidad y la libertad de la persona en relación con el tratamiento de sus datos personales se configura como un derecho positivo que impone obligaciones de hacer a los sujetos obligados a respetarlo.

El primer texto legislativo que reguló los derechos de las personas en relación con el almacenamiento y tratamiento de datos personales fue la Ley del *land* alemán de Hesse del 10 de octubre de 1970. Esta ley reconoció el derecho de los

ciudadanos a controlar el uso que de sus datos personales hacía el Gobierno de ese estado, con la finalidad de evitar los riesgos de que los ciudadanos fueran objeto de una vigilancia permanente por parte de los poderes públicos. Unos años más tarde, en 1977, se aprobó la Ley federal de protección de datos, que incorporó la novedad de extender el ámbito de aplicación de la ley no solo al sector público, sino también al sector privado, de modo que también los sujetos privados que trataran datos personales debían cumplir con las previsiones de la Ley.

En este progresivo reconocimiento de la necesidad de protección de los datos personales frente al tratamiento que realizan tanto los poderes públicos como los actores privados, tiene una especial significación la sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983 sobre la ley del censo, porque supuso la primera elaboración jurisprudencial del derecho de las personas al control sobre sus datos personales, al que denominó «derecho a la autodeterminación informativa» («*Recht auf informationelle Selbsbestimmung*»). Se trata de una sentencia cuya argumentación ha tenido una considerable influencia dado que en ella se encuentran los elementos esenciales de la protección de la privacidad frente al tratamiento de datos.

Lectura recomendada

Hay traducción española de la sentencia en:

J. Schwabe (comp.) (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán* (págs. 94-102). Berlín: Ed. Konrad Adenauer Stiftung.

El Tribunal parte del valor central de la dignidad y la libre autodeterminación de la persona en la Ley fundamental de Bonn. El libre desarrollo de la personalidad garantiza la facultad de las personas de decidir cuándo y con qué límites pueden ser revelados hechos de su vida privada. Esta facultad precisa de especial protección frente al tratamiento automatizado de datos. El almacenamiento masivo de información personal y su tratamiento automatizado permiten generar una imagen más o menos completa de la personalidad de los individuos, sin que el implicado pueda controlar suficientemente su exactitud y utilización. Con ello, las posibilidades de inspeccionar e interferir en la vida de los individuos se amplían de una manera hasta antes desconocida; así, la presión psicológica que supone este control de los datos personales puede influir de manera determinante en el comportamiento de los individuos, coartando su libertad o retrayendo sus posibilidades de acción. Por ejemplo, quien suponga que su participación en una reunión o en una iniciativa ciudadana puede ser registrada por las autoridades y que de ello puede derivarse algún riesgo para él presumiblemente renunciará al ejercicio de esos derechos.

Ante tal riesgo para la libertad de las personas, afirma el Tribunal, un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos sería incompatible con el derecho a la autodeterminación informativa. De este modo, concluye la sentencia, el libre desarrollo de la personalidad presupone, en las modernas condiciones del procesamiento de datos, la protección de los individuos frente a la recopilación, el archivo, el uso y la retransmisión de sus datos

personales. El derecho fundamental garantiza de esta manera la capacidad del individuo para determinar por sí mismo la comunicación y el uso de sus datos personales.

El reconocimiento del derecho a la protección de datos en la legislación y la jurisprudencia alemanas en los años setenta y ochenta constituye un precedente con repercusión en los ordenamientos de otras naciones, así como en el plano internacional. En este último ámbito cabe señalar la iniciativa de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de aprobar en septiembre de 1980 las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, que expresaban el consenso entonces existente sobre los principios que debían regir el archivo y la gestión de la información personal. Estas directrices constituyen una expresión de *soft law*, esto es, se trata de un documento que carece de eficacia jurídica vinculante pero que, por el valor del consenso que expresa, ha influido en la práctica tanto de los Estados como de las organizaciones internacionales, promoviendo la adopción de unos estándares mínimos de protección de la privacidad y los derechos de las personas. En 2013 estas directrices fueron objeto de actualización y revisión.

Referencias bibliográficas

La versión actualizada de las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales puede consultarse en: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Asimismo, el Foro de Cooperación Económica de Asia-Pacífico (APEC) ha adoptado unas Directrices en materia de protección de datos, cuyo contenido se sitúa en línea con las de la OCDE. El documento está disponible en: http://publications.apec.org/publication-detail.php?pub_id=390.

También con un valor declarativo, en el ámbito de Naciones Unidas, cabe citar la aprobación de los Principios rectores sobre la reglamentación de los ficheros computerizados de datos personales por la resolución de la Asamblea General de 14 de diciembre de 1990 (A/RES/45/95).

Referencia bibliográfica

Los Principios rectores sobre la reglamentación de los ficheros computerizados de datos personales están disponibles en: http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf.

El primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos es el Convenio n.º 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 (DCP). Este tratado ha sido ratificado por los 47 Estados miembros del Consejo de Europa y además por otros tres Estados que no forman parte de esta organización regional (Uruguay, Senegal y Mauricio). La finalidad del Convenio, de acuerdo con su artículo 1, es «garantizar [...] a cualquier persona física [...] el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona».

Referencia bibliográfica

En 2010 se inició un proceso de revisión del Convenio n.º 108 que dio lugar a la propuesta de un nuevo texto en septiembre de 2016, que todavía no ha sido aprobado. El texto puede consultarse en: https://rm.coe.int/16806a616c.

El artículo 5 del Convenio, bajo el epígrafe «Calidad de los datos», contiene los principios básicos que debe regir todo tratamiento de datos personales. El citado precepto establece lo siguiente:

«**Artículo 5. Calidad de los datos**

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente.

b) Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades.

c) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

d) Serán exactos y si fuera necesario puestos al día.

e) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado».

De este conjunto de principios se deduce que la licitud de un tratamiento de datos personales depende de que:

- Los datos se hayan obtenido legítimamente, esto es, bien con el consentimiento del particular o bien a partir de una habilitación normativa.
- El tratamiento persiga una finalidad precisa y determinada.
- Los datos obtenidos y tratados sean los necesarios para satisfacer la finalidad del tratamiento y sean exactos.

Estas condiciones impuestas a los tratamientos lícitos de datos parten de la base de que los datos personales objeto de tratamiento deben ser los estrictamente necesarios para conseguir el fin que legitima su obtención y uso. Dicho de otro modo, el principio subyacente en el Convenio es el de que para proteger la vida privada y los derechos de las personas debe minimizarse a lo estrictamente necesario el tratamiento de datos personales. Dado que el tratamiento automatizado de datos es una amenaza para los derechos de las personas, el nivel óptimo de protección, de acuerdo con el Convenio, viene determinado por un principio de minimización del tratamiento.

En la evolución de la regulación del derecho de protección de datos ha tenido una importancia decisiva el derecho europeo. En la década de los noventa se apreció la necesidad de adoptar una normativa que redujera la diversidad legislativa existente en los distintos Estados de la Unión en materia de protección de datos con el fin de facilitar la construcción del mercado interior, de modo que las transacciones comerciales transfronterizas no se vieran dificultadas por tener que cumplir normas nacionales con distintos niveles de protección. Fruto de esa reflexión es 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. Mediante esta directiva se han armonizado las legislaciones nacionales con el fin de que en todas ellas se regulen unas condiciones comunes de la licitud del tratamiento de datos personales.

La Directiva parte de la constatación, según se expresa en sus considerandos, de que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro y pueden constituir un obstáculo para el ejercicio de actividades económicas a escala comunitaria. Para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros. Ahora bien, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección, sino que por el contrario el objetivo es asegurar «un alto nivel de protección dentro de la Comunidad». Por tanto, la Directiva tiene una doble finalidad:

- Contribuir al fortalecimiento del mercado interior eliminando obstáculos al ejercicio de las actividades económicas transfronterizas.
- Garantizar un alto nivel de protección del derecho a la protección de datos en todos los Estados miembros.

Lectura recomendada

Una visión general de la regulación europea en materia de protección de datos puede consultarse en:

H. Burkert (1999). «Privacy-Data Protection: a German/European Perspective». Second Symposium of the German American Academic Council's Project «Global Networks and Local Values», Woods Hole, Massachusetts (págs. 43-69).

En el ámbito del derecho europeo debe señalarse que la Carta de Derechos Fundamentales de la Unión Europea ha incorporado como derecho fundamental en su artículo 8 el derecho a la protección de datos. El derecho se reconoce en los siguientes términos:

«**Artículo 8. Protección de datos de carácter personal**

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

Este precepto establece cinco elementos esenciales del derecho a la protección de datos. En primer lugar, la titularidad corresponde a «toda persona», entendiendo por tal la persona física, pues de acuerdo con la jurisprudencia del Tribunal de Justicia de la Unión Europea las personas jurídicas no son, en principio, titulares de este derecho. En segundo lugar, el objeto del derecho viene constituido por «los datos de carácter personal que le conciernan», esto es, aquellas informaciones, en cualquier formato (escritura, imagen, sonido, etc.), referidas a una persona identificada o identificable.

Un tercer elemento del contenido del derecho viene determinado por los principios que deben cumplirse para que un tratamiento de datos sea lícito, y que en sustancia son los recogidos ya por el Convenio n.º 108 del Consejo de Europa: principio del consentimiento o habilitación legal, principio de finalidad y principio de minimización.

El precepto de la Carta identifica, en cuarto lugar, las facultades básicas que integran el derecho a la protección de datos: el derecho de acceso, esto es, a ser informado sobre qué datos son objeto de tratamiento, por quién y con qué finalidad, así como el derecho de rectificación, que habilita a la persona a exigir la corrección de los datos inexactos. Este derecho de rectificación ha de entenderse complementado con los derechos de cancelación de aquellos datos cuyo tratamiento no resulte lícito y de oposición a aquellos tratamientos que no cumplan los principios. Este conjunto de facultades son conocidas como los derechos ARCO, acrónimo de «acceso, rectificación, cancelación y oposición».

Finalmente y en quinto lugar, el apartado tercero del artículo 8 de la Carta establece el principio de control independiente. Como mecanismo de garantía del derecho a la protección de datos, la Carta exige el establecimiento de una autoridad independiente que vele por el cumplimiento de la normativa de protección de datos por parte de los sujetos públicos y privados.

La regulación contenida en la Directiva ha sido sustituida por el Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, aplicable a partir del 25 de mayo de 2018. Se trata de una norma extensa (contiene 99 artículos precedidos de 173 considerandos), de contenido complejo, cuyas finalidades principales son lograr una homogeneización más intensa del nivel de protección en los distintos Estados –eliminando así los obstáculos todavía existentes a la circulación de datos personales dentro de la Unión– y adaptar la normativa de protección de datos al nuevo entorno tecnológico determinado por la expansión de internet y las redes sociales.

En el plano nacional, la primera regulación del derecho a la protección de datos se realizó por la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD). A pesar de que el artículo 18.4 de la Constitución ordenaba al legislador regular el «uso de la informática» para garantizar los derechos de las personas, el motivo inmediato para aprobar la referida Ley fue la necesidad de contar con una normativa sobre el tratamiento de datos personales como condición para adherirse al Acuerdo de Schengen y al Convenio para la aplicación el Acuerdo de Schengen, que preveían que los Estados parte tuvieran un sistema de protección de datos que cumpliera, como mínimo, con las exigencias del Convenio n.º 108 del Consejo de Europa, convenio que España había ratificado en 1985.

La LORTAD partía de la constatación de que las garantías naturales de la protección de la vida privada derivadas de los factores de tiempo y espacio en el mundo real resultan severamente alteradas por el uso de bases de datos automatizadas que permiten guardar la información por tiempo indefinido y hacerla accesible en cualquier momento. Así se explicaba, muy vivamente, la exposición de motivos de la Ley:

«[...] la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo. Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona. [...] Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas».

Tras la aprobación de la Directiva 95/46/CE, la LORTAD fue derogada y sustituida por la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). El 23 de junio de 2017 el Consejo de Ministros aprobó el anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal que derogará la LOPD, con el objeto de adaptar el ordenamiento jurídico español al RGPD. En el anteproyecto se concretan y desarrollan previsiones que el RGPD ha dejado a la opción de los Estados. Entre las novedades del anteproyecto cabe destacar las siguientes:

Referencia bibliográfica

Puede consultarse el texto del anteproyecto en: http://www.mjusticia.gob.es/cs/Satellite/Portal/es/areas-tematicas/actividad-legislativa/normativa/anteproyectos-informados.

- Se fija la edad de consentimiento de los menores en 13 años.
- Se regula el tratamiento de datos de las personas fallecidas.
- Contiene una regulación específica de algunos tipos de tratamientos de datos (tratamiento de datos de contacto y de empresarios individuales, tratamiento de datos hechos manifiestamente públicos por el afectado, sistemas de información crediticia, tratamientos con fines de videovigilancia, entre otros).
- Se opta por la posibilidad de que la autoridad de control no imponga multas a las administraciones públicas en caso de incumplimiento de la normativa, aunque sí podrá sancionarlas con apercibimiento.

2. La diferenciación del derecho a la intimidad (y la propia imagen) y el derecho a la protección de datos

Luis Javier Mieres

La Constitución española (CE) de 1978 es uno de los primeros textos constitucionales que incorporó al catálogo de derechos fundamentales la necesidad de protección frente al desarrollo y expansión de las bases de datos y su tratamiento automatizado. El artículo 18.4 CE dispone que «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

A diferencia del resto de las garantías que prevé el artículo 18 en sus distintos apartados (derechos al honor, la intimidad personal y familiar y la propia imagen, inviolabilidad del domicilio y secreto de las comunicaciones), en el apartado 4 no se reconoce un derecho fundamental, sino que se establece un mandato al legislador con el objeto de limitar el uso de la informática en garantía de los derechos de los ciudadanos. Esta peculiar estructura normativa del artículo 18.4 CE ha hecho que en la jurisprudencia constitucional se haya tardado más de dos décadas en reconocer la existencia como tal de un derecho fundamental a la protección de datos. La consecuencia de esa tardanza en integrar en el catálogo de derechos fundamentales la protección frente al tratamiento de datos personales ha sido el recurso al derecho a la intimidad como sustituto.

La STC 110/1984 es un buen ejemplo de ello. En esta sentencia se discutía en qué medida la Administración tributaria podía exigir los datos relativos a la situación económica de un contribuyente y, para decidir el caso, tanto el recurrente como el Tribunal Constitucional emplearon como canon el derecho a la intimidad personal. Según el Tribunal, los datos económicos de una persona están protegidos por el derecho a la intimidad si a partir de ellos pueden conocerse hechos pertenecientes a la esfera de la estricta vida personal o familiar del recurrente. De este modo, los datos económicos no son objeto de protección por el derecho a la intimidad por sí mismos, sino solo en tanto que a través de ellos se puede tener acceso a la vida privada de la persona (por ejemplo, sus hábitos de consumo o de ocio).

En esta sentencia el Tribunal ofrece una explicación del reconocimiento del derecho fundamental a la intimidad, que lo vincula al desarrollo tecnológico y que evoca de algún modo el planteamiento de Warren y Brandeis. En efecto, el TC afirma lo siguiente:

«El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respeto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y del desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad».

STC 110/1984, FJ 3.

El caso de la STC 110/1984 es un supuesto típico de tratamiento de datos personales, pero la ausencia en la doctrina constitucional de aquel momento de un específico derecho en esta materia obligó al Tribunal a encauzar el problema planteado como un caso de afectación del derecho a la intimidad.

La primera sentencia en la que el Tribunal Constitucional aborda un caso de tratamiento de datos personales es la STC 254/1993. En el caso, el recurrente había solicitado del Ministerio del Interior si existían ficheros con datos personales suyos, qué finalidad tenían esos ficheros y qué autoridad los controlaba. Frente a la denegación de esa solicitud de información, tras agotar la vía judicial, el particular recurrió en amparo ante el Tribunal Constitucional. En la sentencia, el Tribunal puso de manifiesto que lo que pretendía el recurrente era una prestación de hacer por parte de la Administración, que le diera determinada información, y en este sentido afirmó que «la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)» (FJ 7).

A partir de lo anterior, y empleando el Convenio n.º 108 del Consejo de Europa como criterio interpretativo, al amparo del artículo 10.2 de la Constitución, el Tribunal concluyó que:

«[l]as facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente».

STC 254/1993, FJ 7.

En esta sentencia, de nuevo, la protección de datos se vincula muy estrechamente al derecho a la intimidad, de manera que la garantía para la libertad y la dignidad de la persona frente al uso ilegítimo del tratamiento mecanizado de datos se presenta como una faceta de la intimidad.

El reconocimiento del derecho fundamental a la protección de datos como derecho autónomo y distinto del derecho a la intimidad se produce en la importante STC 292/2000, de 30 de noviembre, que resolvió el recurso de inconstitucionalidad presentado por el Defensor del Pueblo frente a determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El Tribunal destaca, en primer lugar, que el artículo 18.4 CE tiene por objeto un ámbito específico de protección que no se identifica con el del derecho a la intimidad. Esta tesis la apoya en dos razones. Por un lado, la novedad e intensidad de la amenaza para la libertad que supone la informática, que se concreta en que «una persona puede ignorar no solo cuáles son los datos que le conciernen que se hallan recogidos en un fichero, sino también si han sido trasladados a otro y con qué finalidad». Ante este tipo de amenaza, el derecho a la intimidad no aporta «por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico».

Por otro lado, el Tribunal señala la voluntad del constituyente de afrontar tales riesgos de un modo específico, como lo indica el hecho de que un precepto similar al del artículo 18.4 se incluyera en el anteproyecto y que en el debate en el Senado se rechazara la supresión del citado artículo con el argumento de que los derechos del artículo 18.1 no ofrecían garantías suficientes frente a las amenazas que podía entrañar el uso de la informática. En definitiva, «el constituyente quiso garantizar mediante el actual art. 18.4 CE no solo un ámbito de protección específico, sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto» (FJ 4).

Ciertamente, tanto el artículo 18.1 CE como el artículo 18.4 CE tienen un objetivo común: proteger la vida privada de la persona y su reputación, pero en el artículo 18.4 CE, afirma el Tribunal, predomina «una dimensión positiva que excede del ámbito propio del derecho fundamental a la intimidad y que se traduce en un derecho de control sobre los datos relativos a la propia persona» (FJ 5). Este derecho de control conlleva el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley.

Esta diferenciación entre el derecho a la intimidad y el derecho a la protección de datos se proyecta, a su vez, sobre la función, el objeto y el contenido que corresponde, respectivamente, a cada derecho.

En primer lugar, la función del derecho a la intimidad es la de «proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones en contra de su voluntad». En consecuencia, el derecho a la intimidad se traduce en «el poder de resguardar su vida privada de una publicidad no querida». La función del derecho a la protección de datos, en cambio, consiste en «garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado». El derecho se traduce, por un lado, en un poder de disposición sobre esos datos y, por otro lado, «impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información» (FJ 6). Este poder de disposición o control presupone necesariamente, con el fin de que pueda ser ejercido, la posibilidad de que el afectado pueda conocer qué datos poseen terceros, quiénes los poseen y con qué fin.

En segundo lugar, el objeto del derecho a la protección de datos es más amplio que el del derecho a la intimidad. El objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, porque su objeto no es solo la intimidad individual, sino los datos de carácter personal. En particular, son datos sujetos al poder de disposición de su titular también los «datos personales públicos», accesibles a cualquiera. Y en general, los datos de carácter personal protegidos son «todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

En tercer lugar, el derecho a la intimidad tiene un contenido negativo (reactivo), mientras que el de protección de datos personales tiene un carácter positivo (prestacional). En efecto, el derecho a la intimidad «confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido». En cambio, el derecho a la protección de datos integra «un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer» (FJ 6).

Estos poderes y correlativos deberes se concretan en el consentimiento previo para la recogida y uso de datos, el derecho a saber y ser informado sobre el uso y destino de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

El Tribunal concluye su construcción del derecho afirmando que:

> «[...] son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele».
>
> STC 292/2000, FJ 7.

Tras la STC 292/2000 el derecho fundamental a la protección de datos ha quedado perfectamente delimitado en su contenido y diferenciado del derecho a la intimidad.

3. Los tres niveles de protección del derecho a la protección de datos (nacional, europeo y convencional) y sus desarrollos jurisprudenciales

Luis Javier Mieres

Como se ha visto, la garantía del derecho a la protección de datos no se agota en la Constitución. Este derecho también es objeto de tutela por el derecho de la Unión Europea y por sistema convencional del Consejo de Europa.

Todos los poderes públicos del Estado están sometido a la Constitución (art. 9.1 CE), por lo que deben respetar el derecho fundamental a la protección de datos reconocido en el artículo 18.4 CE. Pero además, el Estado español ha ratificado el Convenio Europeo de Derechos Humanos, por lo que está internacionalmente obligado a respetar los derechos garantizados en ese instrumento convencional de acuerdo con la interpretación que establezca el órgano jurisdiccional de garantía, el Tribunal Europeo de Derechos Humanos, que ha reconocido el derecho a la protección de datos como integrante del derecho a la vida privada del artículo 8 del Convenio. Por otro lado, de acuerdo con el artículo 51 de la Carta de Derechos Fundamentales de la Unión Europea, España, como Estado miembro, debe respetar los derechos fundamentales consagrados en esta cuando aplique el derecho de la Unión, por lo que cuando la actuación de los poderes públicos españoles se produzca en aplicación de la normativa comunitaria deberán respetar, entre otros, el derecho a la protección de datos del artículo 8 de la Carta.

En definitiva, existe una concurrencia de normas en la tutela y protección de este derecho. Por ello es relevante deslindar el ámbito de aplicación de cada una y señalar los desarrollos jurisprudenciales más relevantes en relación con cada ámbito normativo.

3.1. La jurisprudencia del Tribunal Constitucional sobre el artículo 18.4 CE

El derecho fundamental a la protección de datos vincula directamente a todos los poderes públicos (art. 53.1 CE), pero su eficacia no se reduce a las relaciones de carácter vertical (ciudadano-poder público), sino que también tiene eficacia horizontal, esto es, es invocable en las relaciones *inter privatos* y, por tanto, los particulares que traten datos personales son sujetos obligados por el derecho fundamental.

Tal y como se ha señalado, el *leading case* en materia de protección de datos es la STC 292/2000, que ha establecido la doctrina general sobre su contenido. A partir de esta sentencia, el Tribunal Constitucional ha tenido la oportunidad de ir desarrollando su jurisprudencia en relación con este derecho fundamental.

Un aspecto que ha sido analizado por el Tribunal Constitucional ha sido el de los límites a la cesión o comunicación de datos personales entre Administraciones públicas. Las Administraciones pueden tratar datos personales bien previo consentimiento de los interesados, bien en virtud de una previsión legal que las autorice a ello, pero en ambos casos ese tratamiento debe estar justificado en una finalidad determinada. Si se ceden o comunican datos personales a otra Administración pública para que los utilice con una finalidad distinta de la perseguida inicialmente, esa cesión será legítima si cuenta con el consentimiento de las personas interesadas o, en su defecto, está autorizada por una ley.

A partir de este criterio, la STC 292/2000 declaró inconstitucional el artículo 21.1 LOPD en la medida en que permitía la cesión de datos entre Administraciones autorizada por una simple norma reglamentaria. Por su parte, la STC 17/2013 ha considerado constitucionales las previsiones contenidas en la Ley Orgánica 4/2000, de 11 de enero, sobre Derechos y Libertades de los Extranjeros en España, introducidas por la Ley Orgánica 14/2003, sobre Cesión de Datos a otras Administraciones Públicas. Así, el TC ha considerado conforme con el derecho a la protección de datos el que la Ley autorice a la Administración General del Estado a conocer y usar datos personales en poder de la Agencia Tributaria, la Tesorería General de la Seguridad Social o del Instituto Nacional de Estadística cuando sean necesarios para el ejercicio de las funciones administrativas en materia de extranjería. Aquí nos encontramos ante un uso de los datos personales para una finalidad distinta de la que originalmente legitimó su tratamiento, pero que no vulnera el derecho fundamental porque la Ley lo autoriza expresamente.

Ahora bien, el TC ha precisado que, cuando no media consentimiento del afectado, para que la cesión o el acceso a los datos por un tercero sean legítimos no basta con que simplemente lo autorice la Ley, sino que la norma legal también debe cumplir con algunos requisitos materiales. En particular, la ley que autoriza una restricción del derecho a la protección de datos debe establecer el límite al derecho de manera clara y precisa y ser conforme al principio de proporcionalidad.

Así, en la STC 151/2014 se analizó la constitucionalidad de algunos preceptos de una ley de la Comunidad Foral de Navarra, que regulaba un registro de médicos objetores a la práctica de interrupciones voluntarias del embarazo. Uno de esos preceptos establecía que a los datos personales contenidos en el registro podrían acceder las personas titulares de la dirección de un centro hospitalario, así como de las direcciones médicas y de enfermería de los hospitales.

La posibilidad de acceso de estas personas fue considerada por el TC como una medida justificada y proporcionada, pues con ello se posibilitaba velar por la debida organización y gestión de la interrupción voluntaria del embarazo, asegurando que al personal médico que había objetado no se le encomendaría la realización de esa prestación sanitaria. En cambio, la previsión contenida en la Ley de que también pudieran acceder a los datos del registro aquellas personas que «autorice expresamente la persona titular de la Gerencia del Servicio Navarro de Salud» fue declarada inconstitucional por el TC porque supone un límite injustificado al derecho a la protección de datos al establecerse en unos términos demasiado abiertos e indeterminados.

Un supuesto que ha merecido una especial atención por parte del TC es el uso de cámaras de videovigilancia en un lugar de trabajo con finalidad de control de la prestación laboral. La captación de la imagen de las personas con el fin de verificar el cumplimiento de las obligaciones laborales constituye un tratamiento de datos personales que, en principio, está legitimado por el artículo 20.3 del Estatuto de los trabajadores, que confiere al empresario el poder de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Ahora bien, un elemento esencial del derecho a la protección de datos es el derecho del afectado de ser informado de la finalidad del tratamiento de datos personales y de quién posee los datos, pues esa información es presupuesto necesario para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. En este punto, en la jurisprudencia se ha planteado el alcance del deber del empresario de informar a los trabajadores de la existencia de un sistema de videovigilancia con finalidad de control laboral.

En la STC 29/2013 se abordó el recurso de amparo planteado por el trabajador de una universidad pública que había sido sancionado por faltas reiteradas e injustificadas de puntualidad, en el que se alegaba que la universidad había utilizado imágenes captadas por las cámaras de videovigilancia instaladas en el recinto universitario con la finalidad de verificar el cumplimiento de las obligaciones laborales sin haber informado previamente de ello al trabajador. El TC consideró que para poder utilizar las imágenes captadas como prueba de las faltas de puntualidad «era necesaria la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral» para la que podían utilizarse las imágenes.

La STC 39/2016, dictada por el Pleno del TC, se ha apartado expresamente del anterior precedente y ha fijado una doctrina más laxa sobre el deber de información. En esta sentencia, la mayoría del Tribunal (tres magistrados formularon voto particular discrepante) consideró que a los efectos de entender satisfecho el derecho de los trabajadores a ser informados sobre la existencia de un sistema de control audiovisual de la prestación laboral, bastaba la existencia en el lugar de trabajo de dispositivos anunciando la instalación de cámaras y captación de imágenes. En el caso se discutía la validez del despido de

una trabajadora de una tienda de una multinacional de ropa por haber venido apropiándose de efectivo de la caja de la tienda en distintas fechas, tal y como se constataba en las imágenes captadas por las cámaras instaladas en el local.

El punto controvertido era que la empresa no había informado específicamente a los trabajadores de que el sistema de videovigilancia de la tienda podía servir, también, para controlar el cumplimiento de los deberes laborales. De seguir el criterio de la STC 29/2013 se hubiera estimado el amparo y declarado la lesión del derecho de la recurrente, pero el Tribunal consideró como suficiente que la empresa hubiera colocado en el escaparate de la tienda el correspondiente distintivo que anunciaba la existencia de cámaras de vigilancia. Por tanto, a partir de esta sentencia, los empleados que trabajen en un lugar en el que existan cámaras de vigilancia y en los que se anuncie su colocación con el correspondiente dispositivo deben asumir que el empresario puede utilizar las imágenes captadas con una finalidad de control de la prestación laboral.

3.2. La jurisprudencia del Tribunal de Justicia de la UE sobre protección de datos

Antes de exponer las líneas jurisprudenciales del Tribunal de Justicia de la UE sobre el derecho a la protección de datos, es importante dejar claro cuál es el ámbito de aplicación de los derechos fundamentales de la Carta respecto de la acción de los Estados.

Al respecto, debe señalarse que han sido dos importantes sentencias de la Gran Sala del Tribunal (sentencia de 26 de febrero de 2013, C-617/10, Akerberg Fransson, y sentencia de 26 de febrero, C-399/11, Melloni) las que han establecido la doctrina sobre el grado de vinculación a los derechos fundamentales de la Carta que es exigible a los Estados, de acuerdo con el artículo 53 de la Carta, cuando actúan dentro del ámbito del derecho de la Unión. Conforme a la doctrina fijada en ellas, cabe distinguir dos situaciones en las que el grado de vinculación será más o menos intenso.

La primera situación se da cuando la normativa europea determina completamente el ámbito de actuación de los Estados miembros, de modo que estos no tienen margen de libertad para introducir ningún tipo de variación. En esta situación, la actividad de los Estados está plenamente sujeta a los derechos de la Carta, que desplazan a los derechos fundamentales nacionales, que no pueden ser invocados para apartarse de lo establecido por la norma europea correspondiente. Esta es la hipótesis decidida en el caso Melloni, en el que el Tribunal afirma que un Estado no puede invocar el derecho a un proceso justo reconocido en su constitución nacional para rechazar la ejecución de una orden de detención europea, más allá de los supuestos taxativamente contemplados en la normativa europea en los que sí se permite rechazar la ejecución de una orden europea de detención. Si la norma europea respeta el derecho

al proceso justo reconocido por la Carta, los Estados no pueden oponer un estándar más alto de protección porque eso supondría minar la primacía del derecho europeo.

La segunda situación es aquella en la que la norma europea no determina completamente la actuación de los Estados, por lo que estos gozan de un ámbito de libertad a la hora de dar cumplimiento al mandato normativo comunitario. De acuerdo con la sentencia Akerberg Fransson, «en una situación en la que la acción de los Estados miembros no esté totalmente determinada por el Derecho de la Unión, las autoridades y tribunales nacionales siguen estando facultados para aplicar estándares nacionales de protección de los derechos fundamentales, siempre que esa aplicación no afecte al nivel de protección previsto por la Carta, según su interpretación por el Tribunal de Justicia, ni a la primacía, la unidad y la efectividad del Derecho de la Unión» (par. 29).

De este modo, en materia de protección de datos, cuando el Estado actúe en un ámbito totalmente reglado por la norma europea, el derecho fundamental relevante es el reconocido en el artículo 8 de la Carta, desplazando así al derecho fundamental nacional previsto, en el caso de España, en el artículo 18.4 CE. En estos casos, la interpretación del Tribunal de Justica sobre el nivel de protección del derecho fundamental a la protección de datos es la que cuenta. Por el contrario, cuando la norma europea deja margen de elección al Estado, el derecho fundamental del artículo 18.4 CE será el aplicable respecto de las normas nacionales en la que se haya concretado la opción legislativa. En este supuesto, la interpretación relevante del derecho fundamental a la protección de datos será la que establezca el Tribunal Constitucional.

El Tribunal de Justicia ha establecido una importante jurisprudencia sobre protección de datos interpretando tanto la Directiva como el artículo 8 de la Carta. Algunas de las sentencias que ha dictado merecen ser destacadas.

En la sentencia Lindquist (C-101/01, de 6 de noviembre de 2003) el Tribunal afirmó que la publicación del nombre de una persona junto con su número de teléfono en una web constituye un tratamiento de datos y que el responsable del tratamiento (el *webmaster*) debe cumplir con las obligaciones establecidas en la Directiva.

En relación con los límites del derecho a la protección de datos, esto es, cuándo resulta legítimo divulgar datos personales, son relevantes dos sentencias. En el asunto Satamedia (C-73/07, de 16 de diciembre de 2008) el Tribunal estableció que la libertad de expresión es un límite al derecho a la protección de datos, de modo que, de acuerdo con el artículo 9 de la Directiva, el tratamiento de datos «con fines exclusivamente periodísticos o de expresión artística o literaria» puede ser legítimo. Al respecto, el Tribunal sostuvo una interpretación amplia de esta excepción, de modo que no se reducía a las publicaciones realizadas en la prensa convencional, sino a través de cualquier otro medio cuya finalidad fuera la comunicación de información al público. Por su parte,

en la sentencia Schecke (C-92/09, de 9 de noviembre de 2010) se consideró que la publicación por una Administración pública de un listado con los nombres de los beneficiarios de subvenciones en materia agrícola, así como de las cantidades recibidas, justificada en una finalidad de transparencia, resultaba desproporcionada, al no quedar acreditada la necesidad de divulgar esos datos personales para asegurar el control de uso de los fondos públicos.

La sentencia ASNEF –Asociación Nacional de Establecimiento Financieros de Crédito– (C-468/10, de 24 de noviembre de 2011) consideró que la normativa española era contraria a la Directiva porque limitaba la posibilidad de un tratamiento de datos sin consentimiento de los afectados, pero amparado en un interés legítimo perseguido por el responsable del tratamiento, a aquellos datos que figurasen en fuentes accesibles al público (esto es, los boletines oficiales, los medios de comunicación o los listines telefónicos). La sentencia estableció, así, que, de acuerdo con el artículo 7.f de la Directiva, cabe tratar datos personales, sin el consentimiento de los afectados, si ese tratamiento es necesario para satisfacer un interés legítimo del responsable del tratamiento, siempre que no prevalezcan los intereses o derechos fundamentales de las personas afectadas.

Una mención especial merece la sentencia Google Spain (C-131/12, de 13 de mayo de 2014), en la que el Tribunal de Justicia reconoció la existencia del llamado «derecho al olvido» frente a los motores de búsqueda. En particular, el Tribunal de Justicia estableció el derecho a que se eliminasen de las páginas de resultados que ofrecía un buscador a partir de las búsquedas del nombre de una persona aquellos enlaces a informaciones que resultasen inadecuadas, impertinentes o excesivas, como consecuencia del paso del tiempo, salvo que existiera un interés público prevalente que justificase mantener la accesibilidad a esa información.

Finalmente, en este breve repaso por la jurisprudencia del TJUE, debe destacarse el asunto Digital Rights Ireland (C-293/12, de 8 de abril de 2014), que declaró la nulidad de la Directiva 2006/24, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, por vulnerar el derecho a la protección de datos reconocido en el artículo 8 de la Carta. El argumento sustancial empleado por el Tribunal fue la vulneración del principio de proporcionalidad en la que incurría la norma europea, pues establecía una obligación general a los prestadores de telecomunicaciones de retener y conservar los datos de los procesos comunicativos a través de telefonía fija, telefonía móvil, acceso a internet o correo electrónico de todos los usuarios. El alcance masivo de la obligación de retención resultaba claramente desproporcionado respecto de la finalidad perseguida (la lucha contra la criminalidad organizada y el terrorismo), pues los datos personales retenidos pertenecían a cualquier persona, aunque no existiera conexión alguna con alguno de aquellos delitos.

3.3. La jurisprudencia del Tribunal Europeo de Derechos Humanos en materia de protección de datos

El Tribunal Europeo de Derechos Humanos (TEDH) es el órgano internacional de garantía previsto por el Convenio Europeo de Derechos Humanos para verificar el cumplimiento de las obligaciones de los Estados de respetar los derechos consagrados en el Convenio y en los protocolos adicionales. De este modo, la jurisdicción del Tribunal se extiende solo a los derechos reconocidos en estos instrumentos convencionales y no abarca el resto de los convenios sobre derechos humanos que se han firmado en el seno del Consejo de Europa, como el Convenio n.º 108 en materia de protección de datos. Por tanto, la jurisprudencia del TEDH solo se refiere a los derechos reconocidos en el Convenio Europeo y en los protocolos adicionales que han incorporado nuevos derechos al texto original, y entre los derechos reconocidos en esos textos no está, de manera expresa, el derecho a la protección de datos.

Lo anterior no significa que el TEDH no haya reconocido la existencia de ese derecho en el marco del Convenio, pero lo ha hecho partir de la interpretación del artículo 8 del tratado que reconoce el derecho al respeto de la vida privada. De este modo, en el ámbito convencional el derecho a la protección de datos no se ha reconocido como un derecho autónomo y separado, sino como una manifestación más del genérico derecho a la vida privada.

El TEDH ha venido sosteniendo una concepción especialmente amplia del derecho a la vida privada, configurándolo como un auténtico derecho-fuente de otros derechos más específicos. Así, el Tribunal ha sostenido que:

> «[...] la noción de "vida privada" es amplia, sin una definición exhaustiva. Abarca la integridad física y moral de la persona. Puede a veces englobar aspectos de la identidad física y social de un individuo. Algunos elementos, por ejemplo, como la identificación sexual, el nombre, la orientación sexual y la vida sexual dependen de la esfera personal protegida por el artículo 8. Esta disposición protege asimismo el derecho al desarrollo personal y el derecho a establecer y mantener relaciones con otros seres humanos y el mundo exterior. Aunque en ningún asunto anterior haya sido establecido que el artículo 8 comportara el derecho a la autodeterminación como tal, el Tribunal considera que la noción de autonomía personal refleja un principio importante que subtiende la interpretación de las garantías del artículo 8».
>
> Sentencia Pretty c. Reino Unido, de 29 de abril de 2002, par. 61.

La doctrina del Tribunal, que concibe el Convenio como «documento vivo» que exige una interpretación evolutiva con el fin de garantizar derechos «reales y efectivos», ha llevado a la jurisprudencia a incorporar en el ámbito de protección del derecho a la vida privada las amenazas que para la libertad supone el uso de las nuevas tecnologías como la informática o los instrumentos de videovigilancia. Así, en relación con la protección de datos, ha afirmado como doctrina general lo siguiente:

«La protección de los datos personales es de fundamental importancia para el disfrute por la persona de su derecho al respeto de la vida privada y familiar, garantizado por el artículo 8 de la Convención. El derecho nacional debe prever garantías adecuadas para prevenir el uso de datos personales contrario a las garantías de ese artículo. La necesidad de tales salvaguardias es mayor cuando se trata de la protección de datos personales sometidos a tratamiento automático [...]. La legislación nacional debería garantizar, en particular, que dichos datos sean pertinentes y no excesivos en relación con los fines para los que se almacenan; y conservados de forma que se permita la identificación de los sujetos de los datos por un tiempo no superior al requerido por la finalidad para la que son objeto de tratamiento que se requiere para el propósito para el cual se almacenan esos datos. La legislación nacional también debe ofrecer garantías adecuadas de que los datos personales conservados están protegidos de manera eficaz contra el uso indebido y el abuso. Las consideraciones anteriores son especialmente válidas en lo que respecta a la protección de categorías especiales de datos más sensibles [...]».

Sentencia S. y Marper c. Reino Unido, de 4 de diciembre de 2008, par. 103.

En la jurisprudencia del TEDH en materia de protección de datos son destacables las sentencias Leander c. Suecia, de 26 de marzo de 1987, Amann c. Suiza, de 16 de febrero de 2000, y Rotaru c. Rumanía, de 4 de mayo de 2000, estas dos últimas de la Gran Sala, en las que se establece que el almacenamiento de datos personales constituye una injerencia en la vida privada garantizada por el artículo 8 del Convenio.

Un ámbito que ha merecido especial atención por el TEDH es el archivo y uso de datos personales en relación con procesos penales. Así, en la ya citada sentencia S. y Marper c. Reino Unido este tribunal consideró que lesionaba el artículo 8 del Convenio la regulación nacional que permitía con carácter general el almacenamiento de las muestras y los perfiles de ADN de personas sospechosas pero no condenadas. Asimismo, en las sentencias M. K. c. Francia, de 18 de abril de 2013, y Brunet c. Francia, de 18 de septiembre de 2014, se declaró la violación del artículo 8 como consecuencia del archivo de las huellas digitales durante un tiempo muy prolongado (en el caso Brunet, más de veinte años) de personas sospechosas pero no condenadas.

En relación con el derecho al acceso a los datos personales objeto de tratamiento, cabe citar la sentencia Gaskin c. Reino Unido, de 7 de julio de 1989, que reconoció este derecho a una persona que pretendía acceder a la información sobre su infancia contenida en los registros de la institución pública que le tuteló. En la sentencia Segerstedt-Wiberg y otros c. Suecia, de 6 de junio de 2006, se consideró que las autoridades públicas suecas no habían lesionado el artículo 8 al negar el acceso a un archivo policial porque la protección de la seguridad nacional, en el caso, constituía un límite legítimo al derecho de acceso.

Finalmente, en relación con la protección de datos sensibles, como los relativos a la salud, son relevantes las sentencias Z. c. Finlandia, de 25 de febrero de 1997, y L. H. c. Letonia, de 29 de abril de 2014, que ponen de manifiesto que en relación con este tipo de datos el grado de protección es más intenso.

4. El futuro de la protección de datos

Luis Javier Mieres

En enero de 1999, el director ejecutivo de Sun Microsystems, Scott McNealy, afirmaba «La privacidad ha muerto. Asúmalo». Una afirmación tan rotunda antes del cambio de siglo, cuando el motor de búsqueda de Google todavía estaba dando sus primeros pasos (inició su actividad en septiembre de 1998) y faltaban cinco años para el nacimiento de Facebook, podía parecer entonces exagerada, pero la evolución de internet y de los servicios de intermediación ha dado lugar a la expansión imparable de la denominada «economía de los datos». La recogida y el procesamiento de datos a una escala sin precedentes impulsan la creación de nuevos productos y servicios. Los datos de cualquier tipo, pero en particular los datos personales, tienen un valor económico innegable y constituyen la base de un sector creciente de actividad económica.

Lectura recomendada

Puede consultarse el artículo que publicó *Wired* sobre el asunto, «SunonPrivacy: "GetOverIt"», en: http://archive.wired.com/politics/law/news/1999/01/17538.

En este contexto de procesamiento masivo de datos resulta paradójico seguir afirmando que uno de los principios fundamentales del derecho de protección de datos es la minimización del tratamiento de datos personales. Pero los riesgos para el libre desarrollo de la personalidad que representa esta revolución tecnológica exigen mantener y reforzar las garantías de la libertad humana amenazada por la vigilancia y el acopio de datos relativos a las personas por gobiernos y empresas. En esta línea, el Reglamento europeo de protección de datos apuesta por reforzar la exigencia del consentimiento como principal fuente de legitimación del tratamiento de datos, al exigir que el consentimiento sea libre, informado, específico e inequívoco, esto es, que el interesado realice una declaración o una acción positiva mediante la que exprese ese consentimiento. Con el Reglamento europeo no cabe deducir el consentimiento del silencio o de la inacción de la persona interesada.

Lectura recomendada

Una visión crítica sobre la eficacia de la normativa europea de protección de datos puede verse en:

B.-J. Koops (2014). «The trouble with European data protection law». *International Data Privacy Law* (vol. 4, núm. 4, págs. 250-261).

Un elemento esencial para la efectividad de la protección de datos es exigir una mayor responsabilidad a las empresas y entidades que tratan datos personales. Por ello el Reglamento parte de la idea de que la vía más eficaz para alcanzar niveles apropiados de protección es imponer a los responsables del tratamiento obligaciones positivas de carácter preventivo, como la denominada protección de datos desde el diseño o por defecto, la adopción de medidas de seguridad, la realización de evaluaciones de impacto sobre la protección de datos, el nombramiento de un delegado de protección de datos o la adopción de códigos de conducta.

La protección de datos es vista por algunos como una rémora que entorpece el desarrollo tecnológico, y que en el nuevo contexto conformado por las tecnologías de la información y la comunicación (TIC) lo que debe reivindicarse es el valor positivo de la transparencia y de compartir información. Ahora bien, buena parte de la utilidad de las TIC, la computación y la automatización depende de la confianza que genera su uso en las personas, y para que los usuarios y destinatarios de los servicios de la sociedad de la información confíen en ello es necesario que tengan la certeza de que sus derechos van a ser respetados. La protección de datos, lejos de estar muerta, tiene un largo recorrido por delante.

Lectura recomendada

Un persuasivo alegato en este sentido puede verse en:

J. Jarvis (2011). *Partes públicas. Por qué compartir en la era digital mejora nuestra manera de trabajar y de vivir*. Barcelona: Gestión 2000.

5. El entramado de normas que regulan el tratamiento de la información personal

Mònica Vilasau

Como ya ha podido constatarse en los apartados anteriores, existe todo un conjunto de normas que regulan el tratamiento de la información personal. No obstante, cabe señalar que, dentro del conjunto de las disposiciones que regulan este aspecto, existen normas que lo hacen de forma directa mientras que otras lo hacen de un modo indirecto. Asimismo, la diversidad de normas, tanto por su origen como por la materia tratada, constituye un abanico muy amplio.

Para tratar de sistematizar un poco el conjunto de las disposiciones aplicables pueden utilizarse distintos criterios. Se considera oportuno en estos momentos recurrir a dos de ellos:

1) En función del origen de las normas y de su ámbito de aplicación, puede distinguirse entre aquellas de naturaleza internacional, las propias de la UE, las de carácter nacional, las relativas a una comunidad autónoma y las de ámbito local.

Como ejemplo de normas de tipo internacional cabe destacar el Convenio n.º 108, de 28 de enero de 1981, los Principios de la OCDE de 1980 (reformados posteriormente) o los Principios de la APEC.

Convenio n.º 108

Se trata del ya mencionado Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este texto fue aprobado el 28 de enero de 1981 y entró en vigor el 1 de octubre de 1985, tras alcanzar cinco ratificaciones. Está disponible en: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

En cuanto a las normas emanadas de la Unión Europera, de entrada conviene subrayar el papel relevante de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2000) y el Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), objeto de estudio detenido en estos módulos.

Referencia bibliográfica

Se puede consultar la Carta de los Derechos Fundamentales de la Unión Europea en la versión consolidada:

Diario Oficial de la Unión Europea (DOUE) C 83 (30 de marzo 2010).

Estos artículos 7 y 8 de la CDFU se dedican, respectivamente, a regular el respeto a la vida privada y familiar y a la protección de datos de carácter personal.

También existen un conjunto de Directivas sobre la materia –a parte de la Directiva 1995/46/CE, derogada por el RGPD–, entre las que cabe destacar:

- Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa al uso del registro de nombres de los pasajeros (PNR).

- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa al tratamiento de datos para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, modificada por la Directiva 2009/136/CE.

Lectura recomendada

Puede consultarse la Directiva 95/46 en:

Diario Oficial de la Comunidad Europea (DOCE) L 281 (23 noviembre 1995).

Directiva 2002/58/CE

DOCE L 201 (31 julio 2002). Esta Directiva derogó la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Directiva 2009/136/CE

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y el Reglamento (CE) n.º 2006/2004, sobre la cooperación en materia de protección de los consumidores. Diario Oficial de la Unión Europea, (DOUE) L 337 (18 diciembre 2009).

Esta directiva a su vez está siendo objeto de reforma para alinearla adecuadamente con la agenda digital. Se inició un proceso de consulta pública que finalizó el 5 de julio de 2016. Al respecto, puede consultarse: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive.

A nivel estatal, los textos de referencia son la LO 15/1999, de Protección de Datos de Carácter Personal (LOPD), y el RD 1720/2007.

A nivel autonómico, hay que tener en cuenta que existen distintas comunidades autónomas que han constituido autoridades de protección de datos y legislado sobre dicha materia. Así, la Agencia Española de Protección de Datos (AEPD: http://www.agpd.es) es la autoridad de control competente de salvaguardar el respeto del derecho fundamental a la protección de datos en lo que se refiere a los tratamientos de datos efectuados por el sector privado y por el sector público en los casos que no queden bajo el control de una autoridad autonómica. Algunas comunidades autónomas, dentro del marco competencial que les otorga la CE, los propios Estatutos de autonomía y la LOPD, han dictado también sus propias normas.

El artículo 41 de la LOPD permite que determinadas funciones de la AEPD, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las comunidades autónomas y por la Administración local, sean ejercidas

por los órganos correspondientes de cada comunidad, que tendrán la consideración de autoridades de control. Basándose en esta habilitación normativa, algunas comunidades autónomas han creado sus respectivas autoridades de protección de datos y la correspondiente normativa que las desarrolla.

La primera autoridad de control autonómica fue la de la Comunidad de Madrid, creada mediante la Ley 13/1995, de 21 de abril, de Regulación del Uso de la Informática en el Tratamiento de Datos Personales por la Comunidad de Madrid, y que fue suprimida con efectos a partir de enero de 2013[1]. En el caso de la Comunidad Autónoma de Cataluña, su Estatuto de autonomía[2] reconoce en el artículo 31 el derecho a la protección de datos personales y su artículo 156 establece las competencias de la Generalitat en materia de protección de datos de carácter personal. Con anterioridad, ya se había creado la Agencia Catalana de Protección de Datos, mediante la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, derogada por la Ley 32/2010[3], que dio paso a la Autoritat Catalana de Protecció de Dades.

(1)La 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid (art. 61) declaró la supresión de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM).

(2)Ley Orgánica 6/2006, de 19 de julio, de Reforma del Estatuto de Autonomía de Cataluña, publicada por el Decreto 306/2006, de 20 de julio, por el que se da publicidad a la Ley Orgánica 6/2006, de 19 de julio, de Reforma del Estatuto de Autonomía de Cataluña.

(3)Se trata de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos (DOGC núm. 5731, de 8/10/2010).

La última autoridad de control autonómica creada fue la vasca, mediante la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

Las Agencias autonómicas tienen encomendada la función de velar por los ficheros de carácter público que existen en sus respectivos ámbitos territoriales.

2) En función del ámbito material, pueden distinguirse aquellas normas que regulan el tratamiento de datos de forma general y aquellas otras que lo hacen de forma específica o sectorial.

En cuanto a las normas de carácter general, destaca sin duda alguna el Reglamento 2016/679, de 27 de abril de 2016, y la Directiva 2016/680 relativa al tratamiento de datos personales en el ámbito penal.

En cuanto a las normas específicas, relativas a ámbitos concretos que afectan directamente a los datos de carácter personal, entre muchas otras cabe destacar aquellas que regulan las bases de datos de ADN, los datos referentes a la salud y a las historias clínicas, o los datos sobre comunicaciones electrónicas.

Ejemplos

Entre otras, véanse: Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de los Derechos y Obligaciones en Materia de Información y Documentación Clínica; Ley 14/2007, de 3 de julio, de Investigación Biomédica; Ley Orgánica 10/2007, de 8 de octubre, Reguladora de la Base de Datos Policial sobre Identificadores Obtenidos a partir del ADN; Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

Junto todo este conjunto normativo que hace referencia de forma directa a la protección de datos, existen otras disposiciones que abordan el tratamiento de la información personal de forma más indirecta. Se trata de normas cuyo

objeto principal no es la regulación del tratamiento de datos, si bien pueden incidir en ello con mayor o menor intensidad. Este seria el caso, entre muchos otros, de la legislación relativa al comercio y a la administración electrónica.

Ejemplos

Entre otras, véanse: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI); Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones; Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos; Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público; Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

Finalmente, dentro del contexto de internet y también en materia de protección de datos, hay que hacer referencia a los elementos de autorregulación que surgen. Se trata de mecanismos de autocontrol que normalmente se darán en el sector privado, pero que no son exclusivos de este ámbito. Constituyen un ejemplo de esta actividad los denominados «códigos tipo», códigos de conducta que pueden acordar un grupo de empresas o las Administraciones públicas a fin de establecer una serie de reglas, condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad o políticas en el tratamiento de los datos personales.

Lecturas recomendadas

Sobre los códigos en general, véase el artículo 18 LSSI, y respecto al caso concreto de la protección de datos, véanse los artículos 32 LOPD y 71-78 RLOPD.

A modo de conclusión

Se ha tratado de hacer referencia a algunas de las principales normas relativas a la protección de datos y a las fuentes de donde emanan. Pero no se debe olvidar que para tratar de resolver los problemas concretos que se planteen debe tenerse en cuenta el ordenamiento jurídico en su conjunto. Ello comporta tener presente disposiciones de diferente naturaleza y rango normativo que regulan los ámbitos en los que incide el tratamiento de la información personal. Por ejemplo, en cuanto al derecho privado, ello puede comportar tener en cuenta normas relativas a defensa de los consumidores, contratación, legislación relativa a menores, derecho bancario y, subsidiariamente, el Código civil, el Código de comercio y la legislación procesal.

Asimismo, en otras ocasiones puede que se planteen conflictos entre distintos derechos fundamentales implicados. Ello exigirá, además de conocer las diferentes normas reguladoras existentes, analizar la jurisprudencia constitucional que los haya interpretado y configurado.

Bibliografía

Agencia de los Derechos Fundamentales de la Unión Europea, Consejo de Europa (2014). *Manual de legislación europea en materia de la protección de datos* [en línea]. Luxemburgo: Oficina de Publicaciones de la Unión Europea. https://rm.coe.int/16806ae663

Burkert, H. (1999). «Privacy-Data Protection: a German/European Perspective» [en línea]. Second symposium of the German American Academic Council's Project «Global Networks and Local Values», Woods Hole, Massachusetts (págs. 43-69). http://www.coll.mpg.de/text/second-symposium-german-american-academic-council%E2%80%99s-project-global-networks-and-local-values-wo

Jarvis, J. (2011). *Partes públicas. Por qué compartir en la era digital mejora nuestra manera de trabajar y de vivir*. Barcelona: Gestión 2000.

Koops, B.-J. (2014). «The trouble with European data protection law». *International Data Privacy Law* (vol. 4, núm. 4, págs. 250-261).

Lucas Murillo de la Cueva, P. (1990). *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática*. Madrid: Tecnos.

Martínez Martínez, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson/Civitas.

Prosser, W. L. (1960). «Privacy». *California Law Review* (vol. 48, págs. 383-423).

Rouvroy, A.; Poullet, Y. (2009). «The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy». En: S. Gutwirth; Y. Poullet; P. De Hert; C. de Terwangne; S. Nouwt (eds.). *Reinventing data protection* (págs. 45-76). Heidelberg: Springer.

Simitis, S. (1987). «Reviewing Privacy in an Information Society». *University of Pennsylvania Law Review* (vol. 135, págs. 707-746).

Villaverde Menéndez, I. (2006). «La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos de carácter personal». En: A. Farriols i Solá (coord.). *La protección de datos de carácter personal en los centros de trabajo* (págs. 48-63). Madrid: Cinca.

Wacks, R. (2010). *Privacy. A very short introduction*. Oxford: Oxford University Press.

Warren, S. D.; Brandeis, L. D. (1890). «The Right to Privacy». *Harvard Law Review* (vol. 4, págs. 193-220). (Hay traducción española de Benigno Pendás y Pilar Baselga: *El derecho a la intimidad*. Madrid: Civitas, 1995).