

La institucionalización de la protección de datos de carácter personal*

María Nieves de la Serna Bilbao

* El presente trabajo se desarrolla dentro del proyecto DER2009-09819 “De los servicios públicos y los servicios de interés general: El futuro de intervención pública en un contexto de crisis económica”, dirigido por el prof. T. Quadra Salcedo.

I. Introducción

Como es sabido, la recopilación y organización de los datos pertenecientes a las personas físicas o jurídicas es una actividad tradicionalmente enfocada tanto al desarrollo del tráfico público como de la actividad privada. Es fácil recordar la existencia de grandes ficheros de distinta naturaleza destinados a acumular datos de las personas, entre los que cabe citar, por ser los más conocidos, a los ficheros de datos fiscales, bancarios, médicos, de solvencia o, incluso, penales. No es posible ignorar, sin embargo, que aquella recopilación y organización de datos personales experimentó un cambio importante tras la aparición de los computadores y la generalización de su uso en toda la población. En efecto, los ordenadores han permitido aumentar de manera exponencial, de forma prácticamente ilimitada, el almacenamiento de datos en los distintos soportes. Este gran adelanto tecnológico —en constante evolución—, sumado a la aparición de Internet, que permite intercomunicar, obtener, difundir y/o apropiarse de los datos personales —sean verídicos o no— por cualquier sujeto, llevó a un replanteamiento total de la regulación jurídica existente, dado que era evidente el peligro que para la intimidad de las personas —en sentido amplio— implicaban tales elementos. En efecto, no cabe duda de que los ordenadores con su gran velocidad de cálculo y los relevantes avances en las telecomunicaciones son herramientas muy importantes para obtener datos personales, recopilarlos, compararlos y contrastar los mismos en un instante.

(...) los ordenadores han permitido aumentar de manera exponencial, de forma prácticamente ilimitada, el almacenamiento de datos en los distintos soportes.

Hoy son indiscutibles las posibilidades ilimitadas que proporcionan estas herramientas tecnológicas para —insistimos— captar, almacenar, relacionar y transmitir todo tipo de datos personales que, enlazados y unidos entre sí, pueden revelar múltiples facetas de la vida de las personas y que, utilizadas por terceros bien intencionados o no, pueden llegar a transformar aquellos datos en una fuente de información muy poderosa, a tal punto de llegar a controlar y presionar a la sociedad causando perjuicios importantes. Muchos han sido los estudios dedicados a esta cuestión, y en ellos se soli-

cita el amparo del derecho para controlar y decidir sobre los datos de cada persona, de tal forma que podamos controlar nuestra intimidad, asegurando, por ejemplo, una calidad mínima de vida de tal suerte que los demás sólo conozcan aquello que cada persona desea compartir y revelar a los otros, sin que por ello se pierda tampoco el control sobre los datos personales. No creemos que el avance tecnológico sea peligroso “*per se*” para la sociedad.

Recordemos que los datos aisladamente considerados pueden carecer de significación intrínseca, pero que, coherentemente enlazados entre sí, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Por el contrario, ciñéndonos a la materia de estudio, la existencia de ficheros de datos personales resulta necesaria e importante para el funcionamiento de la misma al permitir que informaciones relevantes y de gran trascendencia para ésta puedan estar disponibles en momentos cruciales —por ejemplo, los datos de salud cuando se trata de

salvar la vida de las personas—. No obstante esta finalidad quedaría limitada o podría ser perjudicial para las personas si aquellos datos no fuesen exactos, no se encontrasen puestos al día, o si el acceso a los mismos no tuviera unos límites bien definidos. De ahí que el derecho relativo a la protección de datos deba proteger ese ámbito de intimidad, libertad y dignidad, y regular medidas de control sobre los datos —sea de acceso, uso, disposición, modificación, cancelación, como de veracidad, proporcionalidad, finalidad, etcétera—, los usos y destinos de los mismos para evitar poner en peligro la dignidad de las personas. Recordemos que los datos aisladamente considerados pueden carecer de significación intrínseca, pero que, coherentemente enlazados entre sí, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Finalmente, no se puede dejar de mencionar que en la actualidad el derecho a la protección de datos, tal como lo concebimos, no sólo contempla los datos incluidos en los ficheros informatizados —denominados automatizados— sino que también se hace extensivo a los ficheros manuales o en papel —ficheros no automatizados—, en cuanto a que éstos pueden también poner en peligro la libertad, la dignidad o la intimidad en el sentido amplio del término.

II. Un derecho nuevo y en constante evolución

Las inquietudes planteadas en el apartado anterior han dado lugar a la aparición de un nuevo derecho —llamado de tercera generación o de cuarta—⁽¹⁾ que ha ido adquiriendo cuerpo bajo distintas formas tanto en los ordenamientos de los estados democráticos como en las instituciones internacionales.⁽²⁾ Su denominación no es unívoca; en ocasiones se identifica con los conceptos de “*privacy*” en el ámbito norteamericano,⁽³⁾ “*derecho a la autodeterminación informativa*”, en Alemania,⁽⁴⁾ o “*derecho a la protección de datos*”, en el ámbito de la Unión Europea y en la Carta de los Derechos Fundamentales de la Unión Europea aprobada en el año 2000 en su artículo 8.⁽⁵⁾ Además, si bien este nuevo derecho se identifica con una concepción amplia del

Las inquietudes planteadas en el apartado anterior han dado lugar a la aparición de un nuevo derecho —llamado de tercera generación o de cuarta— que ha ido adquiriendo cuerpo bajo distintas formas tanto en los ordenamientos de los estados democráticos como en las instituciones internacionales.

(1) De acuerdo con el profesor Murillo de la Cueva, P.L en “La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, en *El Derecho a la Autodeterminación Informativa*, edit. Fundación Coloquio Jurídico Europeo, Madrid, 2009 págs11 y ss., se denominan así porque “responden a los retos y dificultades de la sociedad de nuestros días. Principalmente, a los derivados del avance tecnológico, del impacto sobre el medio y de las nuevas formas de desigualdad”.

(2) Así, por ejemplo, cabe citar el Convenio 108, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, en 1981, o las numerosas Recomendaciones de la OCDE sobre circulación internacional de datos personales para la protección de la intimidad y la recomendación relativa a la seguridad de los sistemas informáticos de 1980. Sobre los antecedentes del derecho a la protección de datos véase Téllez Aguilera A; *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, edit. Edisofer, Madrid, 2002.

(3) El uso del término *privacy* —que se suele situar hacia 1873, recogido en el artículo “The Right to Privacy” de Warren y Brandeis— proviene de las pretensiones jurídicas de protección de la vida privada para preservar el entorno personal de posibles injerencias no consentidas. Su evolución llevó a que adquiriera en Estados Unidos el rango de Derecho Constitucional en 1965, si bien en sentido amplio del término dentro del derecho a la intimidad. Finalmente, destacar que en Estados Unidos en 1975 se aprueba la Privacy Act donde se recogen los aspectos principales de este derecho. Véase Piñar Mañas, J.L., “La protección de datos: origen, situación actual y retos de futuro”, en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

(4) Término utilizado en la Sentencia del Tribunal Constitucional Federal de Alemania de 15 de diciembre de 1983 relativa a la Ley del Censo. Es preciso destacar al respecto que en Alemania ya se había aprobado la Ley Federal alemana en 1977.

(5) En el año 1992 se inicia la tramitación del proyecto de Directiva de protección de datos que finalmente es aprobada como Directiva 95/46/CEEE. Pero también se encuentran antecedentes anteriores como la Resolución del Parlamento Europeo sobre “La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática”, adoptada 1979. El Tribunal Constitucional Español también hace eco de este término en su célebre sentencia 292/2000, de 30 de noviembre, en donde reconoce y distingue el derecho a la protección de datos del derecho a la intimidad.

derecho a la intimidad, se distingue desde una perspectiva más estricta en tanto que si, ciertamente, el derecho a la intimidad protege la vida privada de las personas —dentro de la que se comprende la familiar, de amistad y de relaciones personales— de cualquier invasión por parte de terceros no autorizados y en defensa de la dignidad, el derecho a la intimidad en sentido estricto tiene como objeto excluir del conocimiento ajeno las intromisiones de terceros en la vida privada de las personas en contra de su voluntad, para lo cual reconoce a su titular una facultad de preservar del conocimiento ajeno nuestra faceta privada.

De esta forma, aquel nuevo derecho se preocupa por fijar reglas objetivas sobre el tratamiento de estos datos, prevé deberes jurídicos para los terceros que se apropien de los datos y establece procedimientos específicos de garantía.

Por el contrario, el denominado derecho a la protección de datos se diferencia del supuesto anterior —derecho a la intimidad en sentido estricto—, en tanto que el bien jurídico subyacente es la libertad informática, valor que persigue, sencillamente, garantizar a cada una de

las personas un poder de control y disposición sobre los datos que les afectan, sean íntimos o no, públicos o privados, para preservar de este modo y, en último extremo, la propia identidad, nuestra dignidad y libertad. De esta forma, aquel nuevo derecho se preocupa por fijar reglas objetivas sobre el tratamiento de estos datos, prevé deberes jurídicos para los terceros que se apropien de los datos y establece procedimientos específicos de garantía. Este derecho también requiere la existencia de una institución pública independiente cuya finalidad es velar por el cumplimiento de las normas que integran este nuevo derecho.⁽⁶⁾ Reconoce así unos derechos y deberes que se erigen en límites impuestos por el legislador al tratamiento de datos por parte de terceros y determina la existencia de normas sancionadoras, penales y administrativas que deben dirigirse a asegurar su plena vigencia. Como destaca Murillo de la Cueva, “los deberes que pesan sobre quienes pretenden tratar información personal, contrapartida de los derechos y de las exigencias de los principios, comportan, junto a su estricto respeto, la observación de formas y procedimientos imprescindibles para hacer efectivas las garantías del derecho de protección de datos”. De esta forma, se puede afirmar que la

(6) Normalmente, se suele considerar la aparición de este derecho a los años sesenta del siglo pasado, cuando se reúne, en el seno del Consejo de Europa, la Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, de donde surge la Resolución 509 de la Asamblea del Consejo de Europa sobre “Los derechos humanos y los nuevos logros científicos y técnicos”.

protección de datos adquiere una sustantividad propia y se define bajo un rótulo nuevo, con una denominación singular que lo identifica, distinta del derecho a la intimidad, en sentido estricto.

Finalmente, corresponde destacar que se trata de un derecho que se encuentra en constante evolución y que, como destaca el profesor Piñar Mañas,⁽⁷⁾ aún continúa perfilándose. Su fundamento radica en la Sentencia de 27 de febrero de 2008 del Tribunal Constitucional alemán, que considera como integrante del derecho a la protección de datos la confidencialidad e integridad de los sistemas tecnológicos de información —dentro de los que se comprenden los ordenadores personales, PDAs, teléfonos móviles—. Esta nueva consideración es debido a que, a través de ellos —solos o interconectados con otros—, se puede acceder a datos personales que expresan la personalidad o aspectos relevantes del comportamiento de las personas, como los correos electrónicos. Por ello, para el citado tribunal, sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro *online*, prohibiendo en consecuencia la utilización de aquellas técnicas en investigaciones de delitos “normales” o en la actividad genérica de servicios de inteligencia.

(...) sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro online (...)

III. El objeto de protección de este derecho “el dato”

Como hemos expresado, el derecho a la protección de datos tiene como objeto de protección el “dato” de una persona física identificada o identificable, aunque algunas legislaciones hayan extendido también su protección a los datos de las personas jurídicas. Por ello, la delimitación de qué se entiende por dato es muy importante, dado que equivale a definir el ámbito de aplicación de las normas sobre protección de datos, es decir, lo que entra o queda fuera de él.⁽⁸⁾

(7) Ob. cit.; pág. 98 y ss.

(8) Véase el artículo de Fonseca Ferrandis, F; “Comentario al artículo 2 de la LOPD”, en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson Civitas, 2010, Madrid, págs. 156 y ss.

Con carácter general, la comprensión del concepto de dato contenida en las distintas normativas vigentes es bastante amplia, definiéndolo como «toda información sobre una persona física identificada o identificable (el “interesado”). A estos efectos se considera identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».⁽⁹⁾ Dentro de esta definición se comprenden distintos tipos de datos como los numéricos, alfabéticos, gráficos,

(...) la comprensión del concepto de dato contenida en las distintas normativas vigentes, es bastante amplia, definiéndolo como «toda información sobre una persona física identificada o identificable (...)

fotográficos, acústicos o de cualquier otro tipo concernientes a personas físicas identificadas o identificables, independiente de que el dato sea íntimo o no, privado o público. Lo importante es que éste, cualquiera que sea, pertenece a una persona concreta, identificada o identifi-

cable y es a ésta a quien el Derecho reconoce un poder de control sobre el mismo y, paralelamente, impone al tercero que se apropia de los datos ciertos deberes jurídicos para que no afecten a los derechos de los titulares, sean éstos fundamentales o no. La amplitud con la que se define el concepto de “datos” determina que dentro del mismo se incluyan todos aquellos que identifiquen o permitan la identificación de la persona, y que puedan servir para la confección de un perfil ideológico, racial, sexual, económico o de cualquier otra índole, o para cualquier otra utilidad y que en determinadas circunstancias constituyan una amenaza para el individuo. Sólo se pueden considerar excluidos del concepto aquellos datos que expresamente la normativa disponga, así como los datos disociados, es decir, aquellos que no permiten la identificación de un afectado o interesado.

(9) Definición contenida en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, aplicada por todos los países miembros de la Unión Europea. En parecidos términos se pronunció la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal*, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, donde se define a los “Datos de carácter personal” como *cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados*. La mención a la citada conferencia es importante dado que tuvo como finalidad definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal así como facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado. También la normativa española, contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Por otra parte, no se puede ignorar que, si bien la amplitud del concepto de “dato” es beneficiosa para los titulares de los mismos —en tanto que “todos” sus datos encuentran protección—, ha supuesto también la existencia —tanto a nivel internacional como dentro de la propia Unión Europea— de cierta incertidumbre. En efecto, aquella amplitud ha determinado la presencia de diversos criterios a la hora de definir el concepto de dato, diversidad que también se ha complicado por la existencia de regulaciones especiales para datos peculiares, como por ejemplo, los datos relativos a salud, telecomunicaciones, laborales, imagen, videovigilancia u otros.

(...) no se puede ignorar que, si bien la amplitud del concepto de “dato” es beneficiosa para los titulares de los mismos —en tanto que “todos” sus datos encuentran protección—, ha supuesto también la existencia —tanto a nivel internacional como dentro de la propia Unión Europea— de cierta incertidumbre.

IV. Características del régimen jurídico de protección de datos

Denominamos características principales del derecho a la protección de datos personales a aquellos elementos que hacen reconocible el derecho y, sin los cuales, el mismo no existe o es violentado. Dentro de estas características son esenciales los principios aplicables a todo tratamiento de datos, los derechos de los titulares de datos, los deberes jurídicos de las personas responsables de ficheros, los terceros que accedan a los mismos, la seguridad de los datos y la existencia de un poder público habilitado para controlar la correcta aplicación de la normativa sobre protección de datos. Veamos todos ellos.

1. Los principios aplicables en todo tratamiento de datos

Existen varios principios reconocidos en el ámbito del derecho a la protección de datos. Todos ellos se encuentran relacionados y ninguno es superior o ejerce una función más importante que los demás. Las clasificaciones sobre los mismos suelen variar de un lugar a otro pero, en definitiva, su contenido suele ser muy similar. En este trabajo reflejaré los más importantes y que nunca pueden dejar de reconocerse para que exista plenamente el derecho a la protección de datos.

En primer lugar, con carácter general, se suele exigir que todo tratamiento de datos de carácter personal se realice de manera “leal” en tanto que no

se produzcan discriminaciones injustas o arbitrarias para el titular del dato. Para ello es necesario que todo tratamiento se desarrolle con plena sujeción y cumplimiento de los principios y fines contenidos en las normativas internacionales existentes, de los derechos y libertades de las personas, y de la normativa vigente de cada país.⁽¹⁰⁾

El principio de finalidad es otro principio esencial en el ámbito de protección de datos e implica que todo tratamiento se debe limitar al cumplimiento de las finalidades determinadas, explícitas y legítimas para las que se ha obtenido el dato. Esto quiere decir que la persona responsable sólo se encuentra habilitada para realizar aquellos tratamientos compatibles con las finalidades para las que obtuvo el dato, a menos, claro está, que obtenga el consentimiento inequívoco del interesado para otras finalidades. El citado principio de finalidad, como ya se apuntó, presenta

El principio de finalidad es otro principio esencial en el ámbito de protección de datos e implica que todo tratamiento de datos se debe limitar al cumplimiento de las finalidades determinadas, explícitas y legítimas para las que se ha obtenido el dato.

una especial importancia en la medida que sirve para valorar la validez de otros principios que rigen en el ámbito de protección de datos como tendremos ocasión de estudiar.

Otro principio intrínseco a la institución analizada es el principio de proporcionalidad que supone que todo tratamiento de datos se debe circunscribir a

aquellos datos que resulten adecuados, relevantes y no excesivos en relación con las finalidades del tratamiento. En virtud de este principio la persona responsable debe verificar que los datos obtenidos y tratados en el fichero sólo sean los necesarios y adecuados al fin con el que fueron obtenidos. En consecuencia, le corresponde minimizar la cantidad de datos de acuerdo con la finalidad perseguida.

El principio de calidad es también esencial en esta materia. Él implica que le corresponde a la persona responsable asegurar que, en todo momento, los datos de carácter personal recogidos y tratados en los ficheros sean exactos, completos, se pongan al día y sean los necesarios para el cumplimiento de las finalidades para las que son tratados. Para lograr cumplir con este principio el responsable debe

(10) Entre las que cabe citar la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos de 1966 y la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal*, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009.

establecer un período de conservación de los datos así como modificar o cancelar de oficio aquellos datos inexactos o que hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento.

Por su relación con el contenido esencial del derecho a la protección de datos es preciso mencionar el denominado principio de transparencia o de información. En efecto, como hemos visto, el derecho a la protección de datos reconoce al titular del dato un poder de disposición sobre los mismos, lo que supone el derecho a conocer quién y para qué obtiene sus datos. Este conocimiento da transparencia al procedimiento de obtención y sólo se cumple si se proporciona antes de obtener el dato, de tal forma que permita conocer todos aquellos extremos necesarios para su control. El principio se cumple si se facilita información sobre determinados extremos tales como la identidad del responsable, la finalidad del tratamiento, los destinatarios a los que prevé ceder los datos de carácter personal, así como la forma en la que los interesados pueden ejercer los derechos reconocidos y cualquier otra información necesaria. Toda la información proporcionada a los interesados debe ser clara, sencilla, entendible y adecuada a la edad del titular del dato —no es lo mismo un menor que un adulto— y, como regla general, se debe facilitar con carácter previo a la recogida o en el mismo momento el que se produce la obtención del dato. El principio se cumple también si los datos no se han obtenido del propio interesado —cuando la norma lo autorice— y la información se facilite a posteriori, dentro de un tiempo prudencial, salvo que resulte imposible o exija un esfuerzo desproporcionado a la persona responsable. Finalmente, es importante destacar —dada la peculiaridad que presenta— que cuando los datos sean obtenidos a través de redes de comunicaciones electrónicas, el principio de transparencia se considera satisfecho si se procede a la publicación de políticas de privacidad, fácilmente accesibles e identificables, que incluyan todos los extremos antes señalados.

Aunque no se trate de un principio propiamente dicho sino más bien de un deber, es necesario mencionar el denominado “deber de secreto” o “deber de confidencialidad” que tiene que regir para todas las personas que conozcan los datos. Se trata de un aspecto muy importante para el correcto funcionamiento de la institución de protección de datos, ya que implica la imposición de la carga

(...) el derecho a la protección de datos reconoce al titular del dato un poder de disposición sobre los mismos, lo que supone el derecho a conocer quién y para qué obtiene sus datos.

de todas las personas —responsables o no— que intervengan en cualquier fase del tratamiento de los datos de carácter personal de respetar la confidencialidad de los mismos. Esta obligación no se agota con la relación laboral o de otro tipo que se haya tenido y haya permitido acceder al dato sino que, por el contrario, continuará vigente aun después de finalizadas aquellas. Téngase en cuenta que no cumplir este mandato puede suponer la vulneración de todo el sistema de protección de datos, por cuanto las personas que acceden a los datos, por la relación existente, son infinitas. Piénsese, por ejemplo, en los datos personales que tiene una empresa y su tratamiento y, aún más, si esa empresa externaliza parte de su actuación. Por ello es un deber que debe respetarse y hacerse cumplir para que la institución de protección de datos pueda ser efectiva.

2. Elementos esenciales del régimen jurídico de la protección de datos

a. Alcance

Como hemos visto, el derecho a la protección de datos supone el reconocimiento a los titulares de los datos correspondientes de un control y un poder de disposición sobre los mismos que se materializa a través de derechos y garantías que, en definitiva, permiten hacer efectivo este derecho. Correlativamente se impone a las personas responsables que obtienen, conservan, tratan, transmiten o ceden datos personales —extensivo a todos los terceros que acceden a los datos, tales como encargados de tratamiento, cesionarios, trabajadores, etcétera—, ciertos deberes jurídicos u obligaciones. Como cierre de aquellos reconocimientos y, para lograr la efectividad de los mismos, las distintas regulaciones exigen la existencia de uno o varios poderes públicos independientes —cuyo número depende de la configuración territorial de cada Estado— que tutelen la correcta aplicación de este derecho.

(...) el derecho a la protección de datos supone el reconocimiento a los titulares de los datos correspondientes de un control y un poder de disposición sobre los mismos que se materializa a través de derechos y garantías que, en definitiva, permiten hacer efectivo este derecho.

Ahora bien, como todo derecho, su reconocimiento no es absoluto y, por tanto, admite un grado de flexibilidad en algunos ámbitos con el fin de lograr

un equilibrio adecuado entre la protección de los derechos del interesado, los posibles intereses legítimos de las terceras personas y el interés público. De ahí la existencia de algunas excepciones al régimen general, excepciones que en todo caso deben encontrar una correcta justificación, adoptada por el legislador y fundamentada en el interés mayor. Con carácter general, en todos los ordenamientos jurídicos se suelen fundamentar dichos límites en la defensa y la seguridad del Estado y en la averiguación de los delitos.

b. Los titulares de los datos

A los titulares de los datos —denominados también afectados— el derecho a la protección de datos, como hemos visto, les reconoce un control y disposición sobre el uso y el destino de los mismos a fin de impedir el tráfico ilícito y lesivo para su dignidad y sus derechos —sean estos derechos fundamentales o no—. ⁽¹¹⁾ Así, a los titulares se les reconoce una facultad de decisión de consentir sobre cuál o cuáles de los datos personales quieren proporcionar a un tercero —poder público o privado— y para qué fin, poder de disposición que también les permite oponerse a la apropiación o uso de los datos por terceros.

Ahora bien, esta regla no es absoluta y puede ser exceptuada siempre que una norma con rango de ley así lo contemple por considerar que prevalece el interés general. En otras palabras, corresponde a los representantes de la soberanía popular permitir excepcionar el control del titular del dato y sustituir su consentimiento. Así, por ejemplo, en el caso de la seguridad o la defensa del Estado o, en otro orden de cosas,

A los titulares de los datos —denominados también afectados— el derecho a la protección de datos, como hemos visto, les reconoce un control y disposición sobre el uso y el destino de los mismos a fin de impedir el tráfico ilícito y lesivo para su dignidad y sus derechos (...)

(11) Existen numerosos estudios que explican la división y, consecuentemente, la diferenciación de estos derechos. Sin ánimo de exhaustividad se pueden consultar los distintos trabajos del profesor Pérez Luño, a “Los Derechos Humanos en la sociedad tecnológica” en vol. *Cuadernos y Debates*, Centro de Estudios Constitucionales, Madrid, 1989, o *La tercera generación de derechos humanos*, Aranzadi, Pamplona, 2006, del Magistrado Pablo Lucas Murillo de la Cueva, en *El derecho a la autodeterminación informativa*, ed. Tecnos, Madrid, 1990; *Informática y protección de datos*, en Centro de Estudios Constitucionales, Madrid, 1993, y del citado autor, conjuntamente con el profesor José Luis Piñar Mañas, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, y toda la bibliografía que allí se menciona.

cuando se permite a las autoridades públicas acceder a datos médicos en casos de epidemias con la finalidad de adoptar medidas inmediatas y preventivas. En estos supuestos prima el interés mayor antes que el particular.⁽¹²⁾

Como regla general, el derecho a controlar los datos implica, pues, para el titular de los mismos la facultad de consentir su obtención o tratamiento, consentimiento que sólo es válido si previamente se le facilita información por parte del

tercero que obtiene los datos. Esta información, como hemos visto, debe tener un contenido mínimo que permita al titular conocer para qué y a quién autoriza su uso. Se trata, en este caso, de cumplir con el principio de información.

El derecho a la protección de datos reconoce también a sus titulares derechos que se configuran, todos ellos, como parte del contenido esencial del mismo. Se trata de los derechos de acceso, rectificación, cancelación y oposición, derechos que permiten al titular del dato controlar los datos y verificar

El derecho a la protección de datos reconoce también a sus titulares derechos que se configuran, todos ellos, como parte del contenido esencial del mismo. Se trata de los derechos de acceso, rectificación, cancelación y oposición, derechos que permiten al titular del dato controlar los datos y verificar en todo momento que cumplen con los principios antes mencionados (...)

en todo momento que cumplen con los principios antes mencionados, en especial con el de calidad. Cada uno de ellos le permite controlar el dato, ya sea conociendo los que están en poder de terceros y sus fuentes de obtención, corrigiendo los mismos a través del derecho de solicitud de rectificación y modificación, solicitando la desaparición del fichero por medio de su cancelación o impidiendo que se lleve a cabo el tratamiento de sus datos de carácter personal o su cese. De esta forma adquiere relevancia, como destaca Murillo de la Cueva, la existencia del “*habeas data*”, institución cualificada activamente por los derechos o facultades que aseguran tal dominio y, pasivamente, por los límites opuestos

(12) En el ámbito español, la Ley Orgánica, 15/1999, de Protección de Datos de Carácter personal concreta que no es preciso el consentimiento cuando se recojan para el ejercicio de las funciones propias de las **Administraciones públicas** en el ámbito de sus competencias; se refieran a las **partes de un contrato o precontrato** de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; tengan por finalidad proteger un **interés vital del interesado** —salud; o cuando los datos figuren en **fuentes accesibles al público** y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero. Sobre el concepto de fuentes accesibles al público, véase de la Serna Bilbao, M.N. “Comentario al artículo 3.j) de la LOPD”, en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson Civitas, 2010.

a quienes desde los poderes públicos o desde la sociedad utilizan información de carácter personal.⁽¹³⁾

c. La persona responsable del fichero

Las personas responsables de los ficheros que obtienen, conservan, tratan, transmiten o ceden datos ajenos se encuentran sujetas, de acuerdo con el derecho a la protección de datos, a unas exigencias formales y procedimentales necesarias para garantizar el cumplimiento de los principios. Dentro de aquellas exigencias y a efectos de que se consideren lícitos los tratamientos, corresponden, básicamente, a las personas responsables los siguientes requisitos:

Las personas responsables de los ficheros que obtienen, conservan, tratan, transmiten o ceden datos ajenos se encuentran sujetas, de acuerdo con el derecho a la protección de datos, a unas exigencias formales y procedimentales necesarias para garantizar el cumplimiento de los principios.

- Utilizar los datos para las finalidades legítimas para las que fueron recabados y con respeto a todos los principios vigentes en materia de protección de datos. En este sentido, debe velar porque el fichero donde se vayan a introducir los datos se haya creado con una finalidad lícita, concreta y determinada y que los datos que allí se introduzcan sean proporcionados a la finalidad, exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Es su responsabilidad adoptar estas medidas.
- En general, antes de tratar un dato debe obtener el consentimiento del titular del mismo, consentimiento que debe ser libre, inequívoco, específico e informado, salvo que se exceptúe su obtención por ley —caso de los datos contenidos en las denominadas fuentes accesibles al público—.
- Finalmente, corresponde a la persona responsable la adopción de medidas de seguridad de forma que impida la manipulación o acceso de los datos por terceros no autorizados o la pérdida de los datos contenidos en los ficheros.

(13) Ob. cit, pág 18.

- En relación con el primer requisito, es preciso indicar que toda persona responsable, que trata datos ajenos, debe realizar tal tarea con pleno respeto a la dignidad de la persona. Por ello y, dado que la verificación de esta vulneración a posteriori no evitaría el daño causado, se exige con carácter previo a la creación de un fichero y antes de introducir datos en el mismo, verificar un control sobre la adecuación y proporcionalidad de los datos y fines por parte de una autoridad independiente, la cual debe llevar un registro público de los mismos. Se persigue de esta manera, por un lado, evitar la proliferación de ficheros y, por otro, controlar el cumplimiento de los principios de protección de datos en el fichero por parte de la autoridad pública habilitada al efecto. Todo ello, insisto, con carácter previo a la recopilación de datos. En consecuencia, corresponde a las personas responsables someter el proyecto de fichero a un control por un poder público independiente —llámese agencia, autoridad o supervisor de protección de datos, u otro— que es el que verifica la relación entre el fin explícito y legítimo perseguido y los datos que se pretende recopilar. Así, se garantiza el cumplimiento “*ex ante*” de todos los principios que rigen en materia de protección de datos, como el de finalidad, de calidad, de proporcionalidad, etcétera.

Por otra parte, cuando los datos de carácter personal objeto del tratamiento deban ser comunicados a un tercero ajeno a la persona responsable para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, el responsable debe velar porque se cuente

(...) cuando los datos de carácter personal objeto del tratamiento deban ser comunicados a un tercero ajeno a la persona responsable para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, el responsable debe velar porque se cuente siempre con el previo consentimiento del interesado, salvo que una ley prevea otra cosa (...)

siempre con el previo consentimiento del interesado, salvo que una ley prevea otra cosa —supuesto típico de la cesión de datos al poder público recaudador de impuestos por parte de todos los sujetos—. Se trata de la institución de la cesión de datos. También puede ser preciso comunicar los datos a terceros con los que el responsable contrate servicios —denominado encargados— en cuyo caso se suele exigir la firma de un con-

trato donde se especifiquen obligaciones para el encargado en aras de respetar el derecho a la protección de datos.

Es preciso indicar que son responsabilidad de la persona a cargo tanto los daños morales como los daños materiales ocasionados a los interesados. Por tal motivo, está obligado a adoptar las medidas necesarias para satisfacer los principios y las obligaciones establecidas por el derecho a la protección de datos. Recordemos en este caso el deber de confidencialidad que pesa sobre todas las personas que accedan a los datos. Es importante que los estados promuevan medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos, judiciales o administrativos, que les permitan obtener la reparación de los daños y/o perjuicios causados, sin desmedro de las sanciones penales, civiles o administrativas previstas, en su caso, por violación de la legislación nacional aplicable en materia de protección de datos.

En cuanto al consentimiento del titular del dato es preciso indicar que la persona responsable debe obtenerlo del titular con carácter previo a la introducción del dato en el fichero. Dicho consentimiento se debe producir por una manifestación de voluntad del titular del dato y no puede existir vicio alguno del consentimiento en los términos regulados por las normas vigentes, es decir, debe ser libre. Por tanto, está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos y los citados datos sólo se pueden recoger para el cumplimiento de finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Igualmente, se debe señalar que el consentimiento del afectado se debe producir para una concreta operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, no caben, por tanto, los consentimientos genéricos. El permiso debe ser también específico y corresponde al responsable del fichero informar al afectado sobre la existencia del tratamiento y las finalidades que se persiguen con el mismo, así como demostrar que ha informado correctamente al interesado y obtenido legalmente la aprobación. La persona responsable no puede deducir el consentimiento por meros actos realizados por el titular de

En cuanto al consentimiento del titular del dato es preciso indicar que la persona responsable debe obtenerlo del titular con carácter previo a la introducción del dato en el fichero. Dicho consentimiento se debe producir por una manifestación de voluntad del titular del dato y no puede existir vicio alguno del consentimiento en los términos regulados por las normas vigentes.

los datos —no cabe el consentimiento presunto—, siendo preciso que siempre exista expresamente una acción u omisión que implique la existencia del consentimiento, siendo en este caso un consentimiento inequívoco.

(...) independientemente de la obligación que pesa sobre la persona responsable, el titular del dato tiene reconocidos los derechos de acceso, rectificación, cancelación y oposición que le permiten controlar todos aquellos extremos.

Cuando el fichero esté creado, corresponde al responsable garantizar el cumplimiento de los principios y, en especial, que los datos contenidos sean exactos y puestos al día de tal forma que respondan con veracidad a la situación

real del afectado, sean estos ficheros públicos o privados y cualquiera sea la finalidad perseguida. Recordemos que, en todo caso, independientemente de la obligación que pesa sobre la persona responsable, el titular del dato tiene reconocidos los derechos de acceso, rectificación, cancelación y oposición que le permiten controlar todos aquellos extremos.

En relación con las medidas de seguridad que el responsable debe establecer y aplicar comprenden las siguientes dimensiones:

- i) Confidencialidad, por medio de la cual se persigue que el sistema sea seguro y concreta el mayor o menor secreto con el que se van a guardar.
- ii) Integridad, que persigue que los datos contenidos en el fichero no puedan ser objeto de alteraciones indebidas, erróneas o no autorizadas.
- iii) Fidelidad, en cuanto que los datos sean reales, exactos y puestos al día de acuerdo con la situación real del afectado.
- iv) Disponibilidad, en virtud de la cual sólo pueden acceder a los datos a aquellas personas autorizadas para ello.

d. Los poderes públicos garantes de la aplicación del derecho a la protección de datos

Con carácter general, las distintas normativas han exigido la creación de entes públicos dotados de una posición de independencia.⁽¹⁴⁾ Algunos autores,

(14) Véase, por ejemplo, la Resolución 45/1990, de 14 de diciembre de la Asamblea General de Naciones Unidas.

como Piñar Mañas se refieren a esta característica como un “principio de control independiente”, principio que considera inherente a la institución de protección de datos en tanto que persigue garantizar la efectividad de dicho derecho. La falta o ausencia de aquel principio en alguna legislación impediría de lleno el cumplimiento del derecho a la protección de datos y, por tanto, lo desnaturalizaría.

A las citadas entidades, para el desarrollo de su función, se les debe reconocer distintas potestades, de control y vigilancia, de tutela de los derechos de las personas, de cooperación o de inspección y sanción, entre otras. Todas ellas persiguen velar por el respeto de todos los principios y derechos que son inherentes al derecho a la protección de datos así como el cumplimiento de todo el conjunto normativo que regula la institución de la protección de datos. Una función de estos organismos que normalmente se suele olvidar es la relativa a la información y la formación. En efecto, esta actividad es, desde mi punto de vista, esencial dado que permite difundir y dar a conocer el derecho a la protección de datos, inculcando buenas prácticas, solventando dudas o problemas que se presentan, formando personal y a los distintos sujetos que intervienen o manipulan datos, elaborando recomendaciones, guías, informes, entre otras, todo ello para la correcta aplicación del derecho.

A las citadas entidades, para el desarrollo de su función, se les debe reconocer distintas potestades, de control y vigilancia, de tutela de los derechos de las personas, de cooperación o de inspección y sanción, entre otras.

Estos organismos, denominados agencias, supervisor, direcciones, etcétera, cuentan con una organización propia y en la que no pueden faltar:

- Los registros de ficheros públicos, cuya función es dar publicidad y conocimiento de los ficheros y tratamientos de datos personales existentes a efectos del ejercicio de los derechos reconocidos.
- Una sección dedicada a proporcionar información y atención de consultas, a efectos de divulgar y solventar las dudas que pueda ocasionar el respeto a la protección de datos.
- Otra dedicada a la inspección, para verificar ante denuncias o sospechas la aplicación correcta de la normativa de protección de datos, actuación que debería ir acompañada de medidas sancionadoras.

V. Conclusión

El derecho a la protección de datos es un nuevo derecho que pretende impedir que los grandes adelantos tecnológicos vulneren nuestra dignidad, libertad e intimidad en sentido amplio. No persigue “prohibir” los avances tecnológicos sino poner “límites” a los usos que dichas tecnologías nos ofrecen. Las tecnologías —ordenadores y telecomunicaciones— permiten el desarrollo de muchas posibilidades para poder obtener infinidad de datos personales y reunirlos de tal forma que no queden aspectos de la vida de

El derecho a la protección de datos es un nuevo derecho que pretende impedir que los grandes adelantos tecnológicos vulneren nuestra dignidad, libertad e intimidad en sentido amplio.

las personas al margen del conocimiento ajeno. De ahí que el derecho a la protección de datos aparezca para proteger facetas de la personalidad de los sujetos al reconocer a las personas el derecho control y disposición sobre sus datos, como

el derecho de acceso, rectificación, cancelación y oposición. Este derecho impone también deberes y concreta aspectos sobre la creación de los ficheros que deben en todo caso estar justificados en una finalidad legítima del titular, así como su uso y utilización y la exigencia de obtener el consentimiento del titular del dato proporcionando información. El no cumplimiento de estos presupuestos es una vulneración importante de los derechos de las personas, sean o no fundamentales. Esta protección se ha extendido también a los ficheros en papel —no automatizados—, en cuanto que éstos pueden también suponer una vulneración a la dignidad de la persona.

Todas las sociedades deben contar con una regulación clara y precisa que reconozca los derechos de los titulares de datos, establezca los principios e imponga deberes jurídicos a los terceros que accedan a dichos datos y les imponga obligaciones y responsabilidades. A estas exigencias se debe sumar la existencia de una institución independiente que garantice el cumplimiento de aquel derecho y su defensa, así como la articulación por parte de los estados de vías administrativas, sancionadoras y judiciales para poder hacer efectivas las reclamaciones que su incumplimiento conlleve.

Como destaca Murillo de la Cueva,⁽¹⁵⁾ todas estas pretensiones se deben justificar a partir de la misma dignidad de la persona y guardan una estrecha

(15) Ob. cit., pág 16.

relación con la libertad que le caracteriza. Libertad individual en su más amplio sentido, concebida como identidad, dado que el uso incontrolado de los datos personales por terceros conlleva riesgos e inconvenientes y lleva a aquellos que se sienten observados y controlados a comportarse de una forma concreta sin poder manifestarse con su propia forma de ser.

Finalmente, no podemos olvidar que se trata de un derecho en constante evolución. Tiene que hacer frente y adecuarse a los nuevos adelantos tecnológicos. De ahí que continuarán apareciendo importantes retos legales y que se presenten ámbitos nuevos por tratar y regular. En este momento es posible citar el “derecho al olvido” que está planteando una verdadera discusión en relación con los buscadores de información en Internet.⁽¹⁶⁾

(16) Véase la Resolución de la Agencia Española de Protección de Datos sobre Google.

Referencias

Resulta imposible citar en este lugar toda la bibliografía existente sobre esta materia

- DAVARA RODRIGUEZ, M.A. *La protección de datos en Europa*, Madrid, 1998.
- De la SERNA BILBAO, M.N. “Comentario al artículo 3.j) de la LOPD”, en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson/Civitas, Madrid, 2010.
- De la SERNA BILBAO, M.N. “La agencia de protección de datos española: con especial referencia a su característica de independiente”, en *Actualidad Informática Aranzadi*, núm. 22, 1997, págs. 1 y ss.
- FONSECA FERRANDIS, F. “Comentario al artículo 2 de la LOPD”, en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson/Civitas, Madrid, 2010.
- MARTINEZ MARTINEZ, R. *Una aproximación crítica a la autodeterminación informativa*, Thomson/Civitas, Madrid, 2004.
- MURILLO DE LA CUEVA, P.L. “La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad”, en *El derecho a la autodeterminación informativa*, edit. Fundación Coloquio Jurídico Europeo, Madrid, 2009.
- PEREZ LUÑO, A. “Los Derechos Humanos en la sociedad tecnológica”, en *Cuadernos y Debates*, Centro de Estudios Constitucionales, Madrid, 1989.
- PIÑAR MAÑAS, J.L. “La protección de datos: origen, situación actual y retos de futuro”, en *El derecho a la autodeterminación informativa*, Fundación Coloquio jurídico Europeo, Madrid, 2009.
- RALLO LOMBARTE, A. *Derecho y redes sociales*; edit Civitas/Thomson; 2010.
- TÉLLEZAGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, edit. Edisofer, Madrid, 2002.
- TRONCOSO REIGADA, A. “Introducción y presentación”, en *Protección de datos personales para Servicios Sanitarios Públicos*, edit. Thomson, Cívitas, Madrid, 2008.
- TRONCOSO REIGADA, A. “Introduction And presentation”, en *An approach to data protection in Europe*. APDCM/Thomson-Civitas, Madrid, 2007, pp. 9-58.
- VIZCAINO CALDERON, M. *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal*, edit Civitas, Madrid, 2001.

-VVAA. *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Director TRONCOSO REIGADA, edit. Thomson/Civitas, Madrid, 2010.

-VVAA, *Comentarios al reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, Directores PALOMAR OLMEDA y GONZALEZ ESPEJO, Thomson/Civitas, Madrid, 2009.

Autora



María Nieves de la Serna

Profesora titular de Derecho Administrativo, Universidad Carlos III de Madrid.

© 2011 Expansiva

La serie **en foco** recoge las investigaciones de la **Corporación Expansiva**, las que tienen por objeto promover un análisis interdisciplinario y riguroso sobre los temas fundamentales de la sociedad actual, con el fin de hacer propuestas que contribuyan a mejorar las políticas públicas del país.

Se agradece la participación de Raúl Arrieta como coordinador del proyecto que dio origen a este documento, así como el apoyo otorgado por el Comité de Retail Financiero. La presente versión fue editada por Daniela Crovetto y tanto ésta como todo el quehacer de Expansiva se encuentran disponibles en www.expansiva.cl

Se autoriza su reproducción total o parcial siempre que su fuente sea citada.