La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud

LUCIA CRISTEA UIVARU

La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud

PRÓLOGO DE

Dra. Carmen Parra Rodríguez

Profesora de Derecho internacional y

Directora de la Cátedra Unesco en Paz, Solidaridad y Diálogo intercultural

Barcelona
2018

BOSCH EDITOR

© ABRIL 2018 BOSCH EDITOR

Librería Bosch, S.L.
http://www.jmboscheditor.com
http://www.libreriabosch.com
E-mail: editorial@jmboscheditor.com

ISBN papel: 978-84-948188-3-7
ISBN digital: 978-84-948188-4-4
D.L: B7233-2018

Diseño portada y maquetación: Cristina Payà (cspaya@sbeditorialdesign.com)

Printed in Spain – Impreso en España

A Sofía, a Jorge, a mis padres y hermano,
cuyo afecto, apoyo, y constante confianza,
han hecho posible la publicación de este libro.

Índice

Prólogo

El mundo cambia a una velocidad vertiginosa influyendo en nuestras vidas, hoy en día nadie se sorprende de recibir noticias que suceden a miles de kilómetros, o de mantener una conversación con un familiar que vive al otro lado del planeta. Basta con introducir un nombre en la red para saber sus datos personales, su profesión y hasta sus hobbies.

Todo esto tiene mucho de positivo ya que mejora las relaciones interpersonales, si bien el problema aparece cuando se pierden los límites de la privacidad y la confidencialidad, siendo utilizados estos datos con fines poco éticos sin que su propietario sea consciente de ello.

Partiendo de estas premisas este interesante libro analiza desde el punto de vista jurídico los riesgos de la sociedad de la información en una materia altamente sensible como es la que se ocupa de la historia clínica de las personas.

Nuestros datos médicos contenidos en un chip dentro de la huella o de la tarjeta digital viajan por la red sin control ya que no existen fronteras que puedan ponerles un límite. Así mismo las recetas médicas ya no solamente quedan escritas en un papel en el consultorio de un hospital, sino que, al ser digitalizadas, quedan desprotegidas y por tanto sin control por parte del paciente. En definitiva, no tenemos poder sobre nuestros datos y ni siquiera tenemos la posibilidad de modificarlos o conocer en su totalidad cuáles de ellos se encuentran almacenados en el ciberespacio.

Por ello es importante leer esta obra en la que su autora, de una forma amena y cercana nos informa exhaustivamente de los riesgos que esto nos puede acarrear al mismo tiempo que nos ofrece soluciones para paliar estos problemas.

Sin embargo, su gran aportación, además de hacer un exhaustivo estudio tanto de los principios que deben inspirar su utilización, como de la normativa, nacional e internacional, en la que quedan contenidos, es la de generosamente utilizar su dilatada experiencia profesional, que le ha permitido detectar donde se encuentran las lagunas, para indicarnos como proteger la vida sanitaria de las personas.

Estos consejos que podemos encontrar a lo largo de la obra no solamente nos previenen del presente, sino que da un paso más allá abordando el Big Data de Salud. Esta herramienta digital se presenta, especialmente en el ámbito sanitario, como un arma de doble filo que puede por un lado mejorar e incluso alargar la vida de las personas, o por otro lado con su mal uso nos puede exponer al abuso de aquellos que pueden manipular algo tan sensible como son nuestros datos de salud.

Conocer los riesgos y actuar sobre ellos es lo que nos propone la autora, gran conocedora de la protección de datos, que utiliza esta obra para plantear y responder preguntas dejando claro que el futuro está abierto y que hemos de aprender de los errores del pasado para no exponer peligrosamente nuestra vida dejándola al alcance de comportamientos carentes de toda ética.

Carmen Parra Rodríguez
Profesora de Derecho internacional y Directora de la Cátedra
Unesco en Paz, Solidaridad y Diálogo intercultural

Introducción

El presente trabajo tiene por objeto el análisis de los problemas jurídicos vinculados y derivados de la incorporación de la historia clínica digital en el entorno sanitario, así como el análisis del cambio de paradigma que se vislumbra en el contexto del Big Data en el ámbito sanitario, que entra en colisión con la protección al derecho de intimidad y la confidencialidad de los datos de salud. El interés de dicho trabajo, viene motivado por la necesidad del reconocimiento del derecho a la protección de datos como un nuevo derecho fundamental en el ámbito normativo, tanto en el ámbito nacional como europeo, carente en la actualidad de una regulación específica, uniforme, consolidada y actualizada.

Para llevar a cabo el análisis de la situación actual, se ha partido inicialmente del estudio de las fuentes normativas referentes a la protección de los datos de salud, tanto en el ámbito de la Unión Europea, como en el ámbito nacional y autonómico, trazando un recorrido legislativo y jurisprudencial que a lo largo de estos últimos 50 años ha venido a configurar a la protección de datos como un nuevo derecho fundamental. Tras el análisis de los diversos ordenamientos sostenemos que es cada vez más notorio el requerimiento de independizar al derecho sanitario y convertirlo en una nueva rama del derecho, por lo que uno de los objetivos de este trabajo será el de ofrecer argumentos que sirvan para acercarnos a esta nueva disciplina jurídica.

Para alcanzar el objetivo de este libro, la investigación se ha desarrollado utilizando diferentes técnicas propias de la investigación jurídica. En primer lugar, desde la observación pragmática y descriptiva del uso de datos, mecanismos de recogida, del tratamiento y acerca de su utilización. En segundo lugar, y desde un punto de vista de investigación, nos centramos en la recopilación y el análisis de la legislación existente en la materia, tanto a nivel europeo como nacional, en el análisis de las diversas opiniones doctrinarias de referencia, en la jurisprudencia, en los informes del Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, y en los informes y resoluciones de las Agencias de Protección de Datos. En tercer lugar, y desde un punto de vista analítico, hemos interpretado si la legislación existente en materia de protección de datos, brinda o no respuesta a la utilización y al tratamiento de los mismos, y, en consecuencia, si salvaguarda nuestros datos personales.

Para obtener resultados el trabajo se ha estructurado en dos partes. La Primera Parte, se divide en cuatro Capítulos. En el primero de ellos, de carácter más introductorio, se parte de la definición de los conceptos objeto del análisis de este libro, identificando cuál es el bien jurídico protegido por el derecho, a fin de poder analizar en profundidad qué es un dato, diferenciándolo de otras imprecisiones terminológicas, acotando el objeto de estudio para centrarnos en el contenido de los datos sensibles poniendo especial énfasis en los datos de salud.

En el segundo Capítulo de la Primera Parte, se realiza un análisis de los elementos jurídicos que vinculan a los datos de salud, analizando los principios jurídicos y éticos, que deben observarse a la hora del tratamiento de ésta categoría de datos, por parte del facultativo médico y del personal sanitario, para explicar los derechos que le asisten al interesado en relación con sus datos de salud y las sanciones que el ordenamiento legal establece en caso de su incumplimiento. Hemos considerado relevante analizar qué se entiende por tratamiento de los datos personales y cuáles son sus límites normativos, porque los datos por sí mismos no constituyen ningún riesgo. Lo que sí goza de amparo normativo es su tratamiento, según tendremos oportunidad de analizar, el hecho de que nuestros datos personales sean tratados por terceras personas conlleva un peligro, y este denominado «tratamiento» es lo que encuentra un paraguas legal y ético que profundizaremos en éste Capítulo.

El tercer Capítulo de la Primera Parte de este trabajo, es el núcleo del mismo, y en él se analizará la integración de los datos de salud, que se encuentran comprendidos en la historia clínica del paciente. En éste Capítulo profundizaremos desde el punto de vista legal, los requisitos que deben observarse en torno a la historia clínica, haremos un breve repaso a su origen, a su definición y a los aspectos que debe reunir, a su contenido, intentando delimitar los parámetros jurídicos que la historia clínica debe respetar, como factor fundamental en la relación médico-paciente. Finalmente, nos centraremos en analizar las diferentes corrientes doctrinarias en torno a la propiedad de la historia clínica, y la relevancia de ésta cuestión.

El Capítulo cuarto de la Primera Parte, resulta de esencial relevancia para el objeto de estudio de esta investigación, y en él nos centraremos en profundizar y analizar desde el punto de vista jurídico y social, a través de la incorporación de las nuevas tecnologías, la evolución que se ha vislumbrado en las últimas décadas en lo referente a las especificidades que la digitalización incorpora en la historia clínica digital, su funcionalidad, los datos que debe contener, las medidas de seguridad que debe respetar y las responsabilidades de los intervinientes en su consulta y redacción. Así mismo haremos referencia a otros documentos digitales, como son la receta digital y la tarjeta sanitaria digital.

En la Segunda Parte del trabajo, en el Capítulo primero, hacemos referencia al cambio de modelo económico y social con respecto al incremento del intercam-

bio transfronterizo de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas, como resultado de la vertiginosa evolución tecnológica y la globalización, siendo éstos elementos los que plantean nuevos retos para la protección de los datos personales tanto a nivel europeo como a nivel nacional.

La Protección de Datos ha surgido como respuesta al desarrollo de la sociedad y frente a la necesidad de la protección legal ante un ámbito absolutamente innovador hace tan solo unos treinta y cinco años. Estos avances requieren un marco más sólido y coherente para la protección de datos en la UE, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Por ello, si la información se refiere a datos de carácter personal, ésta ha de someterse a los principios y a las reglas establecidas, y controlarse de manera eficaz para evitar así una lesión en los derechos de los individuos. Si esa información incorpora además revelaciones sobre datos de salud, las garantías deben ampliarse.

Estas circunstancias llevan a plantearse la necesidad en la uniformización normativa, al menos, en la UE de la que formamos parte, a fin de que dichos avances no resulten vulneradores de un derecho fundamental, como lo es, la protección de datos. En base a ello, y con el fin de avalar un nivel análogo y elevado de protección de las personas físicas por lo que se refiere al tratamiento de los datos personales, debe ser equivalente en todos los Estados miembros, a la vez que se deben superar los obstáculos relacionados con la circulación de datos personales dentro de la UE, el nivel de protección de los derechos y la libertad de las personas físicas, sobre los que tendremos ocasión de profundizar en éste Capítulo.

Asimismo, nos centraremos en el estudio de las circunstancias que han dado lugar a la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y a su análisis. Esta nueva ordenación legal, entrará en vigor el 25 de mayo del año 2018 y derogará la Directiva 95/46/CE. El Reglamento General de Protección de Datos, introduce varias novedades englobadas en un nuevo modelo de protección de datos para Europa. Entre sus previsiones, destaca desde el cambio en la gestión de los datos, al uso responsable de la información. Esto conllevará dar un mayor protagonismo a una figura de nueva creación que es el Delegado de Protección de Datos, en el que recaerá la responsabilidad de determinar y adoptar las medidas que sean necesarias para garantizar la adecuada protección de los datos. Además, el Reglamento introduce en el marco de los datos de salud, dos nuevas categorías, como son los datos biométricos y los datos genéticos. También reformula algunos de

los principios que inspiran la protección de datos e introduce otros nuevos, y realiza otras aportaciones novedosas que estudiaremos en éste Capítulo. Sin embargo, como tendremos oportunidad de exponer, las bases que rigen los ordenamientos normativos vigentes, y el Reglamento General de Protección de Datos, no han resuelto aún la dicotomía entre el derecho a la protección de datos de carácter personal y los avances tecnológicos.

Finalmente, en el Capítulo II de la Segunda Parte, estudiaremos el fenómeno incipiente denominado «Big Data» en el ámbito sanitario, analizando las ventajas que ofrece aunar la información sanitaria dispersa que se dispone de cada paciente y en diversos formatos, agrupándola y organizándola de forma tal, que redunde en el beneficio del paciente, pero también para el sector médico, para la organización hospitalaria, y para las farmacéuticas. Sin embargo, pondremos de manifiesto los inconvenientes que se intuyen en la implementación del Big Data en salud, entre los que destacan la anonimización de los datos que se muestra ajena y no es garantía de la no re-identificación de las personas, creando vulnerabilidad en torno a la información, y la necesidad de que la recopilación, el almacenamiento, el tratamiento y la confidencialidad de los datos sensibles quede garantizada, dotando de mayores garantías jurídicas a la protección de los datos de salud en este novedoso, incipiente pero inevitable entorno tecnológico.

Ciertamente, la información es un bien en sí mismo. Si añadimos a ese «bien» la peculiaridad de que se compone de información personal y sensible de las personas, cobra aún más magnitud. Y si sumamos que la forma de recopilar esos datos sensibles resulta extremadamente sencilla actualmente a través de la utilización de medios electrónicos, entonces es cuando debemos poner el énfasis en conocer con certeza quién recopila esos datos, quién dispone de ellos, para qué fin, y cómo nosotros podemos impedir su utilización para fines que no han sido otorgados a dichos datos. Es en este punto donde la seguridad, el contenido y la manipulación o tratamiento de nuestros datos sensibles cobra máxima importancia tanto en el ámbito legal como social. Y a esta creciente preocupación se añade el factor transfronterizo. Nuestros datos ya no son objeto de las fichas en papel que antiguamente gestionaba la secretaria de un doctor, sino que han pasado a formar parte de bases de datos de grandes servidores que almacenan información, y todo este tráfico de datos trasciende de nuestras fronteras y escapa a un control jurídico en la materia. Si bien la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto de la Ley Orgánica de Protección de Datos 1720/2007, de 21 de diciembre, la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente, y el Reglamento General de Protección de Datos pretenden poner solución a ello, aún sin lograrlo plenamente, el fenómeno denominado Big Data se escapa a la legislación específica existente a nivel nacional y europeo.

PRIMERA PARTE

El derecho fundamental a la protección de datos de carácter sensible

CAPÍTULO I

Aspectos básicos en torno a los datos de salud

SUMARIO: 1. El derecho a la protección de datos. 1.1. El bien jurídico protegido: la intimidad como derecho fundamental. 1.2. Límites normativos marcados por la Protección de Datos en el ámbito sanitario. 2. La búsqueda de la esencia del dato de salud. 2.1. Conjunto de definiciones actuales. 2.1.1. El dato de carácter personal. a) Breves consideraciones sobre la expresión «cualquier información». b) Breves consideraciones sobre la expresión «identificadas o identificables». 2.2. Datos sensibles o especialmente protegidos. 2.2.1. Los datos sensibles. 2.2.2. Los datos relativos a la salud. 2.2.3. Definiciones legales. a) Marco normativo español. b) Marco normativo internacional y europeo. b) 1. Marco jurídico internacional. b) 2. Marco jurídico español.

Introducción

A lo largo de ésta primera parte del libro, y a fin de comprender adecuadamente lo que engloba el dato sanitario, resulta esencial una primera aproximación teórica en la que nos encargaremos de definir los conceptos que van a ser objeto de análisis a lo largo de este trabajo.

Para ello, iniciaremos el estudio del presente apartado analizando brevemente el derecho a la protección de datos y lo que abarca la protección de datos, identificando cuál es el bien jurídico protegido por el derecho, a fin de poder analizar en profundidad qué es un dato, diferenciándolo de otras imprecisiones terminológicas, acotando el objeto de estudio para centrarnos en el contenido de los datos sensibles, poniendo especial énfasis en los datos de salud.

A continuación, expondremos someramente el origen y posterior desarrollo normativo del derecho a la protección de datos, poniendo el acento, en la regulación normativa referente a los datos de salud, tanto en el ámbito internacional como en el

ámbito español, trazando un recorrido legislativo y jurisprudencial que a lo largo de estos últimos 50 años ha venido a configurar a la protección de datos como un nuevo derecho fundamental.

1. El derecho a la protección de datos

La protección de datos es una materia de creación relativamente reciente. Podemos situar como punto de partida legislativo, la década del '60, coincidiendo con el desarrollo de la informática. Es en aquél momento cuando se vislumbra por parte del legislador una preocupación en torno a la protección de la intimidad de las personas.

El derecho a la protección de datos personales se configura en nuestro ordenamiento jurídico como un derecho fundamental en la Constitución Española[1] (en adelante, CE). En el Capítulo Segundo de la CE, donde se asientan los derechos fundamentales y las libertades públicas, tiene especial relevancia el Artículo 18.1 que garantiza el derecho a la intimidad personal. Esto conlleva una protección especial que el legislador asigna a los datos personales de los individuos, que ha servido como punto de partida de la legislación vigente al respecto y de las cada vez más frecuentes sentencias judiciales que los Tribunales se ven obligados a promulgar a fin de preservar este derecho contenido en nuestra Carta Magna, como analizaremos posteriormente.

Los datos personales que ampara el precepto constitucional, son datos absolutamente personalísimos, que sólo pueden pertenecer a un individuo en concreto y por ello podemos definirlo desde dos pilares: por un lado, el derecho a la protección de datos otorga la potestad a la persona cuyos datos pertenezcan a conocer quién tiene información sobre ella, cuál es dicha información, de dónde proviene y para qué finalidad se van a tratar sus datos; y por otro lado, este derecho se configura como el control sobre el uso que se hace de sus datos personales. Este control es lo que nos permite conocer qué datos nuestros se tratan y de qué manera, y ello conlleva a la necesidad de protección jurídica sobre los datos personales.

La terminología utilizada por la protección de datos se refiere de manera amplia al conjunto de normas y principios que regula el tratamiento de datos personales en todas sus etapas, es decir, desde su recolección, almacenamiento, circula-

1 Artículo 18.1, de la Constitución Española de 27 de diciembre de 1978, modificada por reforma de 27 de agosto de 1992 (BOE núm. 207, 28.08.1992).

ción, publicación hasta su transferencia, tanto nacional como internacional[2]. Si bien existen diferencias terminológicas a la hora de la denominación. Así, por ejemplo, MURILLO DE LA CUEVA[3], cuando se refiere a la protección de datos habla del «derecho a la autodeterminación informática», por su parte BAZÁN[4] la denomina «habeas data» y sostiene que:

> Puede conceptuarse al hábeas data como una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter personal[5].

En otras palabras, a través del «hábeas data» el legitimado puede acceder al conocimiento de sus datos personales y al destino de tal información que se encuentre en archivos, registros, bancos de datos u otros medios técnicos, electrónicos, de carácter público o privado, de soporte, y, en determinadas hipótesis (por ejemplo, falsedad o uso discriminatorio de tales datos), se puede solicitar la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos[6].

Por su parte la autodeterminación informativa[7] hace referencia, según SUÑÉ LLINÁS[8], a la decisión personal e intransferible de determinar qué es lo que cada uno de nosotros quiere que los demás sepan de nuestra persona, posibilidad que

---

2 Remolina, N. *Recolección internacional de datos: un reto del mundo post-internet.* AEPD, Madrid, 2015, pp. 96 y ss.

3 Murillo de la Cueva, P. L. *La construcción del derecho a la autodeterminación informática y las garantías para su efectividad.* Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 11-12.

4 Bazán, V. «El Hábeas Data y el Derecho de Autodeterminación Informativa en Perspectiva de Derecho Comparado». *Estudios Constitucionales*. Año 3, núm. 2, Chile, 2005, pp. 85-139. Disponible en Internet: <http://studylib.es/doc/7019100/el-h%C3%A1beas-data-yelderechodeautodeterminaci%C3%B3ninformat> [Consulta: 10 de septiembre de 2016].

5 Bazán, V., op. cit., p. 90.

6 Ibídem.

7 Para profundizar más sobre la conceptualización de «autodeterminación informativa» véase: Murillo de la Cueva, P. L., op. cit., pp. 11-12.; Martínez Martínez, R. *Una aproximación crítica a la autodeterminación informativa. Civitas*, Madrid, 2004, pp. 61 y sig.

8 Suñé Llinás, E. La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina. Tesis presentada en la Universidad Complutense de Madrid, Madrid, 2013, p. 132. Disponible en Internet: <http://eprints.ucm.es/22832/1/T34731.pdf> [Consulta: 17 de septiembre de 2016].

alcanza también al derecho a conocer los datos propios que obran en archivos ajenos y en este punto se relaciona directamente con la protección de los datos de carácter personal, lo que no deriva únicamente en la visión que los demás puedan tener de nuestra persona, sino, yendo más lejos, en la definición de nuestra propia identidad a partir de datos nuestros, que no obstante y por circunstancias de la vida, pudieran ser desconocidos para nosotros. Según refiere, como la protección de nuestro propio ser, de nuestra identidad, de nuestra personalidad[9].

A través de su jurisprudencia[10], el Tribunal Constitucional (en adelante, TC) ha evolucionado desde la concepción del derecho a la intimidad como un límite a la informática, a un nuevo y distinto derecho a la libertad informática, entendido como el derecho a la protección de los datos personales y a la autodeterminación informativa.

El TC, al abordar un asunto vinculado a la protección de datos, sostuvo en la STC 254/93 que:

> Nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales[11].

Asimismo, ya en el año 2000, el TC pondera la protección de datos como un derecho fundamental, diciendo que:

> El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que

9 Ibídem.

10 Entre las más destacadas: STC 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad planteado respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Fundamento Jurídico 7 (BOE núm. 4, 4.01.2001, Suplemento, pp. 104-117); STC 53/1985 de 11 de abril (BOE núm. 119, 18.05.1985); y STC 290/2000, de 30 de noviembre de 2000. Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (BOE núm. 4, 4.01.2001, 70-93).

11 STC 254/1993, de 20 de julio de 1993 del Tribunal Constitucional. Recurso de Amparo núm. 1827/1990 (BOE núm. 197, 18.8.1993).

> por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados 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[12].

Con oportunidad de la STC 292/2000, el TC diferencia, el derecho a la libertad informática del derecho a la intimidad otorgándole una finalidad, un objeto y un contenido propio. Además, saca conclusiones sobre el significado y el contenido del derecho a la protección de datos personales, haciendo un análisis acertado desde nuestro punto de vista, y manifestando que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, al mismo tiempo que permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. Concretamente, determinó la STC 292/2000 que el derecho fundamental a la protección de datos protege cualquier tipo de dato personal, sea o no íntimo manifestando que:

> El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal». Asimismo, añade que: «Pero también el derecho fundamental a la protección de datos

12 STC 290/2000, op. cit.

> posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que, a diferencia de este último, que 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[13].

Pareciera ser que tanto la doctrina, como la jurisprudencia, y las normas, han cambiado las denominaciones, pero, en realidad, cuando se habla de protección de datos o lo que es lo mismo, de «habeas data», hay que entender la referencia a la autodeterminación informativa y viceversa[14].

1.1. El bien jurídico protegido: la intimidad como derecho fundamental

Es imposible hablar de los datos personales sin hacer referencia a su fundamento legal, que, en definitiva, es el bien jurídico que la normativa protege. Su génesis se encuentra en el *derecho a la intimidad*, derecho fundamental reconocido por nuestra CE, como adelantamos. En España, el Derecho a la Protección de Datos es un derecho fundamental, que se articula sobre la dignidad de la persona reconocido en el Artículo 10 de la CE[15], sobre su honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, reconocidos en el Artículo 18[16] de la CE, además de disponer que la ley limitará el uso de la informática para garantizar el honor y a la intimidad.

Con objeto de desarrollar el párrafo 4 del citado artículo 18.4, fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[17] (en adelante, LOPD), que a día de hoy es el eje de la protección de da-

13 STC 292/2000, op. cit.

14 Suñé Llinás, E., op. cit., pp. 132-133.

15 El Artículo 10, de la CE establece que: «*La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social*».

16 El Artículo 18, de la CE establece que: «*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*».

17 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, 14.12.1999). Ésta Ley vino a sustituir la anterior Ley Orgánica 5/1992, de 29 de

tos en España, estando a la espera de la entrada en vigor en mayo del año 2018 del Reglamento General de Protección de Datos, pero que a la fecha de redacción del presente libro aún no es vigente[18].

El concepto jurídico de intimidad, tuvo su origen en un artículo de los juristas WARREN y BRANDEIS[19] en el que se reclamó la necesidad de reconocimiento de un nuevo derecho, denominado derecho a la intimidad. En ese primer momento, éste derecho se configuró como necesario para proteger a la persona frente a las intromisiones de los medios de comunicación. Surgió como la búsqueda de un límite jurídico que vedase las intromisiones de la prensa en la vida privada, para evitar las lesiones que la difusión generalizada de hechos relativos a la vida privada podía provocar. Sin embargo, el derecho a la intimidad debía a su vez limitarse para convivir con otros bienes y derechos fundamentales, como la libertad de expresión y el derecho a la información.

A partir del momento de este reconocimiento legal, el derecho a la intimidad pierde su vertiente más patrimonial para consagrarse como el derecho que posee toda persona para protegerse de las intrusiones ajenas respecto a su vida privada. De éste modo, la libertad individual pasa a ser el fundamento del derecho a la intimidad, que deja de ser un derecho de propiedad, para convertirse en un derecho por sí mismo, el derecho a la protección de datos[20].

Entiende PIÑAR MAÑAS[21] que, el reconocimiento pleno de la protección de datos estriba en que los datos personales son sometidos a tratamiento, lo cual

octubre de regulación del tratamiento automatizado de los datos de carácter personal.

18 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE L 119, 4.05.2016, pp. 1-88).

19 Vid. Warren, S. D.; Brandeis, L. D. «The right to privacy». *Harvard Law Review*. Vol. IV, núm. 5, 1890, pp. 193 y ss.; Pendás, B.; Baselga, P. *Derecho a la intimidad / Samuel Warren, Louis Brandeis*. (Traducción). Civitas, Madrid, 1995.; Westin, A. *Privacy and Freedom.* Athebeum, New York, 1967, p. 7.

20 La primera Constitución que recoge este derecho fundamental fue la portuguesa en el año 1976, donde en su Artículo 35 hacía referencia a «dato» para luego ser modificada en el año 1982 y ampliar el concepto a «datos personales», y finalmente en el año 1989 dotar de más protección al derecho. Para profundizar más sobre el tema, véase: Troncoso Reigada, A. *La protección de los datos personales. En busca del equilibrio.* Tirant lo Blanch, Vol. 1, Valencia, 2010, pp. 49-50.

21 Piñar Mañas, J. L. *Legislación de Protección de Datos.* Iustel, Madrid 2011, pp. 34-35.

implica que se tratan datos ajenos, y que los mismos deben utilizarse con estricto respecto a los derechos del interesado. Es por ello, que, el legislador le otorga la máxima protección porque, en definitiva, estamos hablando de la dignidad humana. En el mismo sentido, SUÑÉ LLINÁS[22] entiende que el carácter primordial reside, en realidad, en la autodeterminación informativa, verdadero derecho fundamental que enlaza en la esencia misma de la dignidad humana. Por su parte, GARRIGA DOMÍNGUEZ[23] sostiene que la Ley de Protección de datos pretende proteger la propia personalidad del individuo, de forma mediata a través de la posibilidad inmediata que el individuo tiene sobre la información que le concierne, posibilitando su control.

Recientemente, el Magistrado SALCEDO[24], Presidente de la Sección 9ª de la Audiencia Provincial de Barcelona, ha manifestado en el marco del 1r Congrés de l'Advocacia de Barcelona que: «*El derecho a la intimidad es una derivación del derecho a la dignidad. Y por ello, el referido derecho a la intimidad ha venido a construirse como un derecho propio y que es necesario para mantener una calidad de la vida humana*». Prosiguió el Magistrado haciendo una reflexión muy importante: «*la intimidad es un derecho a ser desconocido, lo cual constituye las lindes de nuestra vida privada*». Por lo tanto, y consecuentemente con lo esgrimido por SALCEDO[25], se genera un doble deber, por un lado, el deber jurídico de abstención, y, por otro lado, el deber jurídico de no hacer uso de lo conocido.

Sostiene al respecto, HERRÁN ORTIZ[26] que:

> Si bien es cierto que el derecho a la protección de datos nace vinculado a la idea de intimidad, ha de superarse esta concepción y avanzar en el reconocimiento de un nuevo derecho fundamental, que en la actualidad se configura a partir de la atribución de un haz de facultades de actuación y control que permiten a la persona decidir sobre la información que le concierne.

22 Suñé Llinás, E., op. cit., p. 134.

23 Garriga Domínguez, A. *Tratamiento de datos personales y derechos fundamentales.* 2ª Edición, Dykinson, Madrid, 2009, p. 53.

24 Salcedo, A. (30.06.2016) El delicte de revelació de secrets: especial menció a l'aportació de documents en procediments judicials. Ponencia celebrada en el marco del 1r Congrés de l'Advocacia de Barcelona, celebrado el 30 de junio de 2016, ICAB, Barcelona. Disponible en Internet: <www.congresadvocaciabcn.cat> [Consulta: 1 julio 2016].

25 Ibídem.

26 Herrán Ortiz, A. I. *El derecho a la protección de datos personales en la sociedad de información.* Universidad de Deusto, Instituto de Derechos Humanos, Bilbao, 2003, p. 21.