MIGUEL MARCOS AYJÓN

Prólogo de
ESTEBAN MESTRE DELGADO

La **protección de datos** de carácter personal en la **justicia penal**

JYB
BOSCH PENAL

Esta monografía analiza la repercusión de la normativa sobre la protección de datos de carácter personal en todos los ámbitos de la jurisdicción penal en España. La investigación se circunscribe al campo penal y, particularmente, al ámbito geográfico de nuestro país, sin perjuicio de las referencias a la situación en Europa u otros países de nuestro entorno. Se pueden distinguir tres aspectos diferenciados de la materia objeto de estudio:

- En la primera parte se desarrollan los principios generales del derecho a la protección de datos y, especialmente, aquellos que más interesan a la Justicia penal. Estamos ante un novedoso derecho fundamental con una rápida evolución normativa y jurisprudencial.

- La segunda parte se refiere al análisis de la protección de datos en el ámbito judicial y, más concretamente, a su gestión por los Juzgados y Tribunales, describiendo los diversos ficheros sobre los que se apoya la labor jurisdiccional, así como el tratamiento que se realiza de los datos personales.

  En esta parte también se examina el ámbito estrictamente procesal, aquel relativo a la recogida de datos durante la instrucción y enjuiciamiento, especialmente en la aportación de pruebas con el máximo respeto a los derechos fundamentales de la persona. También los aspectos relacionados con la comunicación e información a las partes de los datos contenidos en el proceso judicial. Mención especial merece todo lo relativo al intercambio de información, la cooperación judicial penal en el ámbito internacional y la protección de datos.

- La tercera y última parte contiene un estudio exhaustivo de los delitos que protegen el derecho a la protección de los datos de carácter personal y que castigan el tratamiento indebido de los mismos. Se realiza un análisis de los preceptos penales que lo protegen, comenzando con los antecedentes legislativos, las reformas posteriores a la entrada en vigor del Código Penal, la regulación en el derecho comparado, así como el bien jurídico protegido. Posteriormente, y siguiendo la estructura de la teoría jurídica del delito, se estudian los elementos objetivos del tipo de injusto, el elemento subjetivo, los subtipos agravados y atenuados, las causas de exclusión de la antijuridicidad y la culpabilidad, el *iter criminis*, la autoría y la participación, así como las circunstancias modificativas de la responsabilidad criminal.

El libro finaliza con la exposición de las conclusiones, la bibliografía utilizada y la jurisprudencia analizada.

BOSCH PENAL

ISBN: 978-84-121579-3-2

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LA JUSTICIA PENAL

MIGUEL MARCOS AYJÓN

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LA JUSTICIA PENAL

PRÓLOGO DE
Esteban Mestre Delgado
Catedrático de la Universidad de Alcalá

Barcelona
2020

BOSCH EDITOR

© ABRIL 2020 BOSCH EDITOR

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

ISBN papel: 978-84-121579-3-2
ISBN digital: 978-84-121579-4-9
D.L: B 5349-2020

Printed in Spain – Impreso en España

Índice

SEGUNDA PARTE

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y LA ADMINISTRACIÓN DE JUSTICIA

TERCERA PARTE

EL DELITO CONTRA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO VII

CAPÍTULO VIII

Abreviaturas

ADN:	Ácido desoxirribonucleico.
ADPCP:	Anuario de Derecho Penal y Ciencias Penales.
AEPD:	Agencia Española de Protección de datos.
AEAT:	Agencia Estatal de la Administración Tributaria.
AN:	Audiencia Nacional.
AP:	Audiencia Provincial
ARCO:	Derechos de acceso, rectificación, cancelación o supresión y oposición.
Art:	Artículo.
BDGS:	*Bundesdatenschutzgesetz,* Ley Federal de protección de datos alemana, Ley de 14 de enero de 2003. Debe tenerse en cuenta que el *Buntestag* aprobó el 27 de abril de 2017 una nueva Ley que entró en vigor el 25 de mayo de 2018.
BOC:	Boletín Oficial del Congreso.
BOE:	Boletín Oficial del Estado.
C:	Constitución Española
CCAA:	Comunidad Autónoma.
CE:	Dentro de la expresión Directiva 95/46/CE, se refiere a Comunidad Europea.
CEE:	Comunidad Económica Europea.
CENDOJ:	Centro de Documentación Judicial dependiente del CGPJ.
CEJ:	Centro de Estudios Jurídicos de la Administración de Justicia, dependiente del Ministerio de Justicia.
CGPJ:	Consejo General del Poder Judicial
CP:	Código Penal.

CTEAJE:	Comité Técnico Estatal de la Administración de Justicia Electrónica.
DNI:	Documento Nacional de Identidad.
DOUE:	Diario Oficial de la Unión Europea.
DPDUE:	Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo de 2016), relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
DPO:	Delegado de Protección de datos (*data protection officer).*
DRAE:	Diccionario de la Real Academia Española de la Lengua.
DUEPNR:	Directiva de la Unión Europea 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo de 2016), relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y delincuencia grave.
ECRIS:	Sistema de intercambio de información sobre antecedentes penales dentro de los países de la Unión Europea.
ed.:	Edición.
EEUU:	Estados Unidos de América.
EJIS:	Esquema judicial de interoperabilidad y seguridad.
EUROJUST:	Unidad de Cooperación Judicial de la Unión Europea.
EUROPOL:	Agencia Europea de Policía.
EOMF:	Estatuto Orgánico del Ministerio Fiscal.
FD:	Fundamento de Derecho.
INFTC:	Instituto Nacional de Toxicología y Ciencias Forenses
INT:	Interior, cuando se refiere a Orden INT, es una Orden Ministerial del Ministerio del Interior.

JAI:	Consejo de Justicia y Asuntos de Interior (Consejo de la Unión Europea). Cooperación policial y judicial en materia penal. Se utiliza para referencia la normativa europea sobre la materia (2008/977/JAI del Consejo)
JUS:	Justicia, cuando se refiere a Orden JUS, es una Orden Ministerial del Ministerio de Justicia.
FGE:	Fiscalía General del Estado
LDAP:	Protocolo simplificado de acceso a directorios (*Lightweight Directory Access Protocol*).
LEC:	Ley de Enjuiciamiento Civil.
LECR:	Ley de Enjuiciamiento Criminal.
LEXNET:	Sistema de comunicaciones electrónicas regulado en el RD 1065/2015.
LIBE:	Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo.
LO:	Ley Orgánica.
LOGP:	Ley Orgánica General Penitenciaria.
LOPD:	Anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal. (BOE de 14 de diciembre de 1999), derogada por la disposición derogatoria única de la LO 3/2018.
LOPDGDD:	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE de 6 de diciembre de 2018).
LOPJ:	Ley Orgánica del Poder Judicial.
LORPM:	Ley Orgánica Reguladora de la Responsabilidad Penal de los Menores. Ley Orgánica 5/2000.
LORTAD:	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. (BOE de 31 de octubre de 1992) y derogada por la LOPD.
LPL:	Ley de Procedimiento Laboral.
nº:	Número.
NIE:	Número de identidad de extranjero.

OCDE:	Organización para la Cooperación y el Desarrollo Económico.
op. cit.:	Obra citada.
OLAF:	Oficina Antifraude de la Unión Europea.
p.:	Página.
PCPP:	Proyecto de Código Procesal Penal de 2013.
PNJ:	Punto Neutro Judicial.
PNR:	Registro de nombre de pasajeros de las compañías aéreas. (*Passenger name record*).
pp:	Páginas.
Pte:	Ponente.
RAA:	Reglamento de Aspectos accesorios del Consejo General del Poder judicial 1/2005.
RCDS:	Registro Central de Delincuentes sexuales.
RCP:	Registro Central de Penados.
RCPVDG:	Registro Central para la Protección de las Víctimas de Violencia doméstica y de género.
RCRC:	Registro Central de Rebeldes Civiles.
RCSFM:	Registro Central de Sentencias Firmes de Menores.
RD:	Real Decreto
RDL:	Real Decreto ley.
REAJ:	Registro electrónico de apoderamientos judiciales.
Rec:	Recurso
RLOPD:	Reglamento que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Real Decreto 1720/2007, de 21 de diciembre (BOE 19 de enero de 2008).
RP:	Reglamento Penitenciario aprobado por RD 190/1996, de 9 de febrero (BOE de 15 de febrero de 1996).
RPDUE:	Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (DOUE de 4 de mayo 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 de Protección de Datos de la UE).
S:	Siglo.
Sr:	Señor.
Sra:	Señora.
ss:	Siguientes.
SAN:	Sentencia de la Audiencia Nacional.
SAP:	Sentencia de la Audiencia Provincial
SIRENE:	Oficina para la petición de información adicional en la Parte Nacional del Sistema de Información de Schengen (*Suplementary Information Request at the National Entry*).
SIRAJ:	Sistema de registros administrativos de apoyo a la administración de Justicia regulado en RD 95/2009, de 6 de febrero (BOE 7 de febrero de 2009).
SITEL:	Sistema Integrado de Interceptación de Comunicaciones Electrónicas.
SJP:	Sentencia del Juzgado de lo Penal
SSAP:	Sentencias de las Audiencias Provinciales.
SSTC:	Sentencias del Tribunal Constitucional de España.
SSTEDH:	Sentencias del Tribunal Europeo de Derechos Humanos.
SSTJUE:	Sentencias del Tribunal de Justicia de la Unión Europea.
SSTS:	Sentencias del Tribunal Supremo de España.
STC:	Sentencia del Tribunal Constitucional de España.
STEDH:	Sentencia del Tribunal Europeo de Derechos Humanos.
StGB:	*Strafgesetzbuch,* Código Penal alemán.
STSJ:	Sentencia del Tribunal Superior de Justicia.
STS:	Sentencia del Tribunal Supremo de España.
STJUE:	Sentencia del Tribunal de Justicia de la Unión Europea.
TC:	Tribunal Constitucional.
TEDH:	Tribunal Europeo de Derechos Humanos.

TFUE:	Tratado de Funcionamiento de la Unión Europea, publicado en el Diario Oficial de la Unión Europea el 30 de marzo de 2010.
TIC:	Tecnología de la información y de la comunicación, Abreviatura utilizada para referirse a las nuevas tecnologías relacionadas con la informática y las telecomunicaciones.
TJUE:	Tribunal Justicia de la Unión Europea.
TS:	Tribunal Supremo.
UE:	Unión Europea.
Vid:	Véase.

Prólogo

Por ESTEBAN MESTRE DELGADO
Catedrático de Derecho Penal
Universidad de Alcalá

I

Nunca en la historia de la Humanidad se han generado, transmitido y almacenado más datos que en la actualidad. Y ello por la confluencia (recíprocamente autoalimentada) de tres realidades de muy reciente aparición: el desarrollo tecnológico, la proliferación y expansión social de los instrumentos de comunicación y de tratamiento y almacenamiento de la información, y un relevante cambio de mentalidad, que prioriza la extimidad, como factor de relación social, sobre el valor, históricamente preponderante, de la intimidad.

Esta transformación instrumental y de mentalidades ha sido tan relevante que, si en el siglo pasado Ortega y Gasset llegó a sintetizar que «yo soy yo y mi circunstancia», en este siglo XXI Duportail ha reubicado esa conclusión, afirmando que «nuestra vida digital es nuestra verdadera vida».

Los efectos valiosos de este nuevo contexto vital son incuestionables, y se reflejan en todos los ámbitos de la vida: permiten la adquisición instantánea de información sobre cualquier persona, lugar o tema que se desee conocer; facilitan la comunicación y el intercambio de noticias y opiniones entre personas geográficamente muy distantes; agilizan extraordinariamente el manejo de archivos y bases de datos profesionales y laborales; dinamizan la búsqueda, selección y contratación de bienes y servicios, con independencia de la distancia física que pueda existir entre los contratantes; y enriquecen de manera exponencial las relaciones interpersonales.

Pero también existe una perspectiva negativa. Prácticamente cada día se descubren y ponen en práctica nuevos mecanismos de agresión electrónica o cibernética (esencialmente contra la intimidad, la propia imagen, el honor, la libertad e indemnidad sexuales o el patrimonio), que además se llevan a efecto con cada vez más perfeccionados sistemas de encriptación o enmascaramiento de autoría. Son comportamientos que en otro lugar he calificado como alevosos, pues, al mismo

tiempo que potencian la efectividad de esas dinámicas agresivas (en muchas ocasiones delictivas), minimizan los riesgos de descubrimiento o identificación de sus autores. Y, de este modo, la comunidad alegre y confiada de los usuarios de internet resulta cada día más frágil, más vulnerable y más expuesta a actuaciones cada vez más sofisticadas. Así, por ejemplo, en la actualidad nadie puede estar seguro de sus secretos (captables por cualquier sistema de espionaje o de interceptación de las comunicaciones), ni de su propia identidad (que cualquiera puede suplantar fácilmente para cargar sus compras en una tarjeta de crédito ajena, o para solicitar un préstamo bancario, garantizado con un inmueble propiedad de un tercero), ni del patrimonio (pues los depósitos bancarios abiertos pueden transferirse sin que lo autorice, ni lo sepa siquiera, su titular). Los ejemplos más dañinos son los que afectan a los menores, que utilizan con toda confianza las redes sociales, sin percatarse (hasta que terminan enredados en la trama) de que pueden ser observados y engañados por interlocutores que no se corresponden, en realidad, con las apariencias que muestran sus mensajes.

Y la sociedad no es plenamente consciente de estos enormes riesgos que derivan de estas nuevas tecnologías, y de su utilización cotidiana en los más diversos ámbitos ciudadanos, y por los más variados (en tipologías e intenciones) usuarios.

II

Ante este nuevo panorama de conflictos personales, con evidente trascendencia social, surge de nuevo la necesidad del Derecho, de las reglas jurídicas que, en garantía de los bienes jurídicos e intereses individuales (y a veces colectivos), regulan los usos de esas nuevas tecnologías, disciplinando conductas, diseñando límites, determinando prohibiciones, y, en caso de incumplimiento, imponiendo sanciones. Cuatro son los ámbitos más comprometidos en esta tarea:

a) El marco, general y superior, lo establece el artículo 18 de la Constitución que, plasmando previsiones normativas supraestatales de inexcusable observancia, y empleando conceptos ampliamente compartidos por ello en los ordenamientos jurídicos de nuestro contexto cultural, garantiza el derecho a la intimidad personal y familiar, y al secreto de las comunicaciones, e impone que la ley ha de limitar el uso de la informática para garantizar esa intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos. Se elevó así al máximo rango normativo, incorporándole en el núcleo duro de los derechos fundamentales (y otorgándole la mayor protección y proyección que la Constitución ofrece), el reducto de priva-

cidad personal que cada ciudadano excluye del conocimiento de terceros, y cuyo contenido en la actualidad pone en valor el derecho de control de la persona sobre sus propios datos, abarcando también las facultades del habeas data, o derecho a la autodeterminación informativa, como expresión del derecho a controlar el uso de los datos personales insertos en programas informáticos, que habilita para articular oposición a que sean utilizados con fines distintos a aquel para el que fueron obtenidos, generando un haz de facultades que se han calificado como «libertades informáticas». Aún más, en este libro que ahora principia habla su autor del «derecho fundamental a la protección de datos», que consiste en un poder de disposición y control sobre los datos personales que faculta a la persona a ejercer dos facultades diferenciadas: Decidir cuáles son los datos personales propios de los que puede disponer, o puede recabar, un tercero, en qué circunstancias y con qué límites (que es la facultad que se identifica con la denominada «autodeterminación informativa», y que se concreta jurídicamente en consentir o denegar la recogida y obtención de datos, y su posterior tratamiento, uso y cesión a terceros); y ejercer el conjunto de derechos que conforman la «identidad informática» de una persona, y que permiten una defensa global del derecho fundamental a su intimidad. Esos derechos tienen por objeto saber en todo momento quién dispone de esos datos personales y a qué uso los somete (lo que conlleva al derecho a estar informado de la inclusión de los datos en un fichero, archivo o banco de datos); a acceder a esos datos personales; a oponerse a esa posesión y uso; a rectificar los datos erróneos; a la supresión de determinados datos sensibles; a la cancelación de los datos, y fijación de su validez temporal; y a la exactitud y pertinencia de los datos, así como a su confidencialidad (de forma que se garantice la adopción de medidas para que personas no autorizadas no puedan acceder a los datos personales).

b) El Código Penal es la segunda gran norma de protección de los derechos individuales (y colectivos) frente al uso abusivo de las nuevas tecnologías, ya que la delincuencia informática y cibernética están experimentando un crecimiento exponencial porque la comisión de infracciones penales a través de los ordenadores tiende a asegurar su resultado, minimizando los riesgos que pueden derivar para el agresor de la relación personal con la víctima; porque la realización de estas infracciones optimiza en términos exponenciales la eficacia del esfuerzo criminal (tanto en términos de daño como de rentabilidad); y porque la ejecución de estos delitos busca su impunidad a través de la ocultación de sus autores por los anchos dominios de la aldea global (la world wide web). Son las que en alguna ocasión he denominado «las tres leyes del cibercrimen».

La respuesta estatal frente a esa dinámica delictiva es constante, como demuestran las Leyes Orgánicas 1/2015, de 30 de marzo (que ha incorporado, como nuevos instrumentos de represión de la delincuencia informática y cibernética, los delitos de child grooming, de difusión de imágenes concernientes a la intimidad personal, de interceptación de transmisiones no públicas de datos informáticos, y de daños informáticos) y 1/2019, de 20 de febrero (que ha reforzado las previsiones de utilización de internet o las tecnologías de la información y comunicación para la comisión de un delito de abuso de mercado).

c) La Ley de Enjuiciamiento Criminal es el tercer pilar esencial de este ámbito defensivo. Su reforma por Ley Orgánica 13/2015, de 5 de octubre («para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica»), ha ampliado, intensificado y, desde luego, actualizado (tecnológicamente hablando), las ya numerosas facultades de investigación de los delitos que esta norma tradicionalmente otorgaba a los Jueces de Instrucción, dando una nueva y más eficaz regulación de las diligencias de «comprobación del delito y averiguación del delincuente» (Título V del Libro II de la Ley), que permitiesen que el Estado dispusiera de los mismos mecanismos de lucha contra el crimen que los que emplean quienes lo cometen. Así, junto a las tradicionales previsiones de «la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen», o «la intervención de las comunicaciones telefónicas del procesado», la Ley de Enjuiciamiento Criminal dispone ahora de una regulación específica, amplia y detallada, para la interceptación de las comunicaciones telefónicas y telemáticas [artículo 588 ter, apartados a) a m)], para la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos [artículo 588 quater, apartados a) a e)], para la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización [artículo 588 quinquies, apartados a) a c)], y para el registro de dispositivos de almacenamiento masivo de información [artículo 588 sexies, apartados a) a c)]. Además, y en cláusula segura de cierre del sistema, el artículo 588 octies garantiza la conservación de los datos por terceros, que pueden ser expresamente requeridos para ello por la Policía Judicial o el Ministerio Fiscal.

Este elenco de nuevas medidas de investigación, aplicables sólo en supuestos legalmente tasados, posibilita actuaciones de un alcance y eficacia impensables hace muy poco tiempo: la escucha y grabación de las conversaciones que mantenga un investigado desde cualquier terminal y medio de comunicación, así como las de la víctima (cuando fuera previsible un grave riesgo para su vida o integridad), e incluso las que pueda desarrollar un tercero (si bien ello tan sólo cuando exista constancia de que el investigado se sirve de sus