LA PROTECCIÓN DE DATOS EN EL ORDENAMIENTO EUROPEO Y EN ESPAÑA

D. Miguel Marcos Ayjón

Secretario Judicial, profesor asociado de la Universidad CEU San Pablo y profesor tutor de la UNED

Resumen: La protección de los datos personales es un derecho fundamental reconocido en nuestra Constitución y en el ámbito de la Unión Europea. La proliferación de las nuevas tecnologías aumenta la preocupación sobre la utilización de nuestros datos personales, y la sociedad presiona para que el ordenamiento jurídico regule una respuesta adecuada y proporcionada a la nueva realidad. En el presente artículo se hace un estudio de la normativa de la Unión Europea al respecto, de la normativa española, así como de su protección penal y de la necesidad de ser incorporada a proceso penal español.

Abstract: The protection of personal data is a fundamental right recognized by Spanish and European Union laws. The proliferation of new technologies has increased the concern about the use of personal data. Therefore, society is demanding an adequate legal system which provides a response to the new reality. In this study both

European Union and Spanish legislation regarding this aspect are studied, as well as criminal protection and the need to be incorporated this protection into Spanish criminal proceedings.

1. Introducción

Cuando recuerdo una de las obras literarias que más me han hecho reflexionar y me han causado sensación, sin duda, lo fue la novela de GEORGE ORWELL «1984», considerada por muchos la mejor obra literaria del S. XX.

En la obra se dibujan, dramáticamente, bajo la trama y la anécdota de «1984»: la relación entre la técnica y la naturaleza, las posibilidades de una manipulación técnica del ser humano y la influencia de la técnica sobre la política. A este respecto conviene evocar uno de los pasajes del libro cuando le dice uno de los miembros supremos del partido al protagonista: «*La naturaleza humana la creamos nosotros. El hombre es un ser infinitamente maleable*».

Sin duda, lo que más llama la atención del autor, es la gran imaginación de recrear un mundo dominado por un Gran Hermano que todo lo controla gracias a la técnica, que todo lo ve, lo domina y manipula para conseguir una meta superior, aquella que determinan los miembros supremos del partido único o del Estado.

Esta realidad ficticia, recreada a finales de los años 40 del pasado siglo, comienza a ser real en el año 2013 debido a la tecnología. La informática, internet, las telecomunicaciones, las cámaras de seguridad, las bases de datos, son avances que producen un cambio sin precedentes en la forma de vida, en las relaciones sociales y, por tanto, en el campo jurídico.

Algo similar sucede en el derecho penal. Junto con los tradicionales delitos que son recogidos en los códigos penales desde principios del S. XIX en los países de nuestro entorno; como son: el homicidio, las lesiones, el robo, la estafa o la falsedad documental; surgen nuevos ilícitos penales como la estafa informática, el *phising, el pharming, el child grooming* o ciberacoso, o la pornografía infantil en la red.

La proliferación de delitos al calor de las nuevas tecnologías, especialmente a través de internet, no es una predicción o un futurible para años venideros, es una realidad que tenemos hoy en día en los juzgados y tribunales, con una clara tendencia a incrementarse exponencialmente debido al uso cotidiano de las redes de comunicación, la facilidad de quebrantar la ley en el anonimato de la persona

y los beneficios económicos que pueden obtenerse rápidamente sin apenas riesgo.

Uno de los problemas que acarrean las nuevas tecnologías es la facilidad para confeccionar potentes bases de datos que permiten almacenar información sobre un conjunto de individuos para después utilizarla con finalidades sociales, comerciales, laborales, políticas o, incluso, delictivas.

Es fácil imaginar lo que supondría para una compañía aseguradora conocer la información médica de los ciudadanos, para las entidades bancarias saber aquellas personas que no pagan sus deudas y conocer su patrimonio real, para las compañías automovilistas descubrir aquellas personas que han superado recientemente las pruebas del carnet de conducir y conocer sus gustos personales.

También la propia alteración de las bases de datos en perjuicio de terceros, como introducir a una persona en un registro de morosos sin que tenga deuda alguna, o atribuir a una persona unos antecedentes penales que no tiene.

Como ocurre siempre en el derecho penal, la realidad supera a la ficción y son múltiples los delitos que pueden cometerse al albur de la recopilación, almacenamiento, explotación y comercialización de los datos personales.

En la actualidad, la Unión Europea debate un nuevo marco jurídico que establezca el necesario equilibrio entre el desarrollo de las nuevas tecnologías, incluido Internet, y el respeto a la privacidad y los datos personales. Este equilibrio precisa de unas cautelas o normas especiales en el ámbito del proceso penal, en el que las nuevas técnicas de investigación sean lo suficientemente innovadoras para afrontar nuevos fenómenos delictivos pero, al mismo tiempo, han de respetar los derechos fundamentales de los sospechosos e imputados, incluido su derecho a la privacidad y la protección de datos personales.

Las modificaciones introducidas en la normativa general sobre protección de datos (la propuesta de Reglamento sobre protección de datos, que sustituirá a la actual Directiva 95/46/EC) podría afectar a un gran abanico de empresas que deben modificar su estrategia comercial, especialmente a la hora de comercializar los datos para uso publicitario, y reforzar la seguridad para evitar las fuertes multas ante posibles grietas. Es el caso de Google, que ha sido llevado por las autoridades españolas de protección de datos al Tribunal de Justicia de la UE, es un buen ejemplo de la tensión entre el desarrollo de las nuevas tecnologías y la protección de la privacidad de los ciudadanos.

En el ámbito del proceso penal, la tensión es también evidente. La necesidad de contar con una regulación adecuada en este ámbito específico ha llevado a la Comisión a proponer una Directiva específica sobre intercambio de información en el ámbito policial y judicial que pretende regularlo, no sólo en casos de intercambio de información entre distintos Estados Miembros, sino, también en el marco de procesos penales nacionales.

En este trabajo se realizará una breve exposición en la que especificarán los conceptos básicos que deben conocerse sobre la materia, los derechos y principios contenidos en la protección de datos, el contenido de la actual normativa europea y hacía donde se dirige y, por último, cual es la regulación española, especialmente en el ámbito penal y procesal con una breve referencia al ámbito administrativo.

2. La protección de datos de carácter personal. Conceptos básicos

Con antelación al análisis de la normativa sobre la protección de datos personales, conviene hacer una breve referencia a los conceptos básicos que son utilizados en esta materia con la finalidad de una mejor comprensión de la regulación objeto de estudio.

Para ello, vamos a utilizar como ejemplo los datos que se recogen cuando un alumno realiza la matricula de la universidad.

a) DATO PERSONAL: Es el concepto sobre el que gira toda la normativa, utilizándose este término para designar la información relativa al sujeto que le identifica o singulariza, según el art. 3 de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), se trata de cualquier información concerniente a personas físicas identificadas o identificables.

   En el ejemplo de la matriculación en la Universidad de un alumno, se refiere a su nombre, apellidos, edad, sexo, fecha y lugar de nacimiento, documento nacional de identidad o pasaporte, residencia, estudios que realiza, asignaturas de las que se matricula y cuantos datos sean requeridos por la Universidad para la admisión.

b) PERSONA AFECTADA O INTERESADO: Se trata de la persona física titular de los datos personales que son objeto de tratamiento. En nuestro supuesto sería el alumno que realiza la matricula.

c) TRATAMIENTO: El término se refiere al procesamiento de los datos, es decir, las actividades a las que se someten los datos personales. Incluye cualquier actividad desarrollada sobre los datos personales, desde la recogida, grabación, conservación, modificación, bloqueo y cancelación, así como las cesiones, consultas, interconexiones y transferencias de datos.

   Cuando se realiza una matriculación de un alumno se realiza, la Universidad recoge una serie de datos personales para después grabarlos en un fichero que los conserva. Posteriormente, se pueden realizar múltiples actividades con ellos, desde una consulta, hasta el análisis y estudio de los alumnos matriculados según sus características (por sexos, edades, procedencia, residencia, etc.).

   Se conoce como fichero al conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso.

d) RESPONSABLE DEL TRATAMIENTO: Es la persona física o jurídica responsable del tratamiento o procesamiento de los datos personales y, por tanto, responsable de la correcta aplicación de las normas sobre protección de datos.

   Sin duda, en el ejemplo que estamos utilizando, el responsable del tratamiento es la Universidad.

   Es muy frecuente que el responsable del tratamiento no realice directamente el tratamiento de los datos personales, sino que delega esta función en otra persona que procesa los datos por cuenta del responsable, a quien se le denomina ENCARGADO DEL TRATAMIENTO. Podría ser una Facultad concreta de la Universidad o un Departamento o la Biblioteca.

   Cuando distintas personas procesan la misma información separadamente; por ejemplo: un auxiliar administrativo, el profesor o el bibliotecario; cada una de estas personas es el *data controller* o responsable de los datos que maneja.

e) CONSENTIMIENTO DEL INTERESADO: Toda manifestación de voluntad libre, inequívoca e informada previamente, mediante la que el interesado consienta el tratamiento de los datos personales que le concierna.

   Antes de realizar la matricula, se nos informa en el impreso o en el portal *web* de que los datos van a formar parte de un fichero que está registrado en la Agencia de Protección de Da-

tos. Cuando se firma la matricula se realiza el consentimiento para el tratamiento de los datos.

f) CESIÓN DE DATOS: Cualquier comunicación o revelación de los datos a una persona distinta del interesado.

Cuando la Universidad comunica nuestros datos de una forma legal a la Consejería de Educación u otra entidad relacionada con la actividad educativa.

g) DATOS SENSIBLES: Algunos datos personales se consideran especialmente sensibles como: el origen racial o étnico, ideología, afiliación sindical, religión u otro tipo de creencias, salud, vida sexual, etc. Estos datos gozan de mayor protección y se acompañan de ciertas garantías para su tratamiento.

3. Principios, derechos y procedimientos

La normativa sobre protección de datos se articula en torno a tres grandes categorías: los principios sobre protección de datos, los derechos de la persona a la cual se refieren, y los procedimientos para la protección y salvaguarda de tales principios y derechos, incluida la protección penal. Estas normas se aplican a los datos personales almacenados en cualquier tipo de fichero estructurado que permita obtener información sobre una persona en particular, según el art. 2 de la Ley Orgánica de Protección de Datos (LOPD), no se aplica a actividades personales o domésticas, materias clasificadas, investigación sobre terrorismo o delincuencia organizada, régimen electoral, finalidad estadística, la derivada del Registro Civil y de Penados y Rebeldes. A pesar de ello, alguno de estos registros (como el de antecedentes penales actualmente integrado en el sistema de registros administrativos de la Administración de Justicia) se remite a esta normativa para someterse a sus reglas.

La protección abarca a cualquier tratamiento automatizado de los datos personales, independientemente del soporte en el que se recojan y, por lo tanto, a cualquier dato contenido en el soporte papel, ordenadores, teléfonos móviles, cámaras digitales, circuitos cerrados de televisión o equipos de grabación.

I. Principios

Estas normas incluyen unos principios para el procesamiento o tratamiento de los datos que deben ser respetados en todos los casos por

el responsable del tratamiento. Se trata de unas garantías que deben seguir todos los responsables y encargados del tratamiento y cuyo incumplimiento conllevará una serie de sanciones. Se trata de los siguientes:

1. Los datos deben ser procesados de manera lícita y legal.
2. Los datos deben ser almacenados con una finalidad específica y legítima, y no de una forma incompatible con dicha finalidad.
3. Los datos deben estar en proporción con la finalidad para la que son recogidos y tratados, es decir, adecuados y relevantes para tal fin y, por tanto, no excesivos.
4. Los datos deben ser exactos y actualizarse cuando sea necesario.
5. Los datos no podrán permanecer en un fichero más allá del tiempo necesario para el cumplimiento de la finalidad para la que fueron recogidos.
6. El responsable del tratamiento debe garantizar la seguridad de los datos, adoptando las medidas técnicas y organizativas para ello, y en proporción a la naturaleza de los datos y el nivel de daño que pudieran causar.

II. Derechos

La persona afectada o interesado goza de una serie de derechos, los más importantes son:

— Conocer si sus datos personales son objeto de tratamiento.

— El acceso a los datos personales que son objeto de tratamiento.

— Se puede solicitar la rectificación, bloqueo o borrado de los datos si éstos no son precisos o no están siendo procesados de acuerdo con la ley.

— Se puede oponer al tratamiento de los datos si concurren ciertas circunstancias que lo justifiquen.

— El tratamiento de los datos personales requiere el consentimiento del afectado, salvo que la ley disponga otra cosa (art. 6 LOPD).

III. Procedimientos

Por último, es preciso destacar que cada Estado cuenta con una autoridad supervisora en materia de protección de datos cuya princi-

pal competencia es la de asegurar el cumplimiento de la normativa. Es una autoridad plenamente independiente y debe supervisar el tratamiento de los datos que se lleva a cabo por las autoridades gubernativas y de cualquier entidad pública, así como el realizado por las autoridades privadas.

En nuestro país es la Agencia de Protección de Datos (AEPD) y tiene capacidad de llevar investigaciones sobre el procesamiento de datos, de solicitar al responsable del tratamiento que adopte las medidas pertinentes, de imponer sanciones y compensaciones económicas por los perjuicios ocasionados. También puede poner en conocimiento de las autoridades judiciales la vulneración del derecho fundamental a la protección de datos, así como los delitos cometidos al respecto.

Los responsables del tratamiento deben notificar a la autoridad de supervisión los ficheros creados y el tipo de tratamiento que se pretender llevar a cabo. Los ciudadanos pueden presentar sus dudas y reclamaciones sobre el tratamiento de sus datos personales ante la autoridad de supervisión.

Las autoridades de supervisión de los distintos países miembros de la Unión Europea cooperan entre sí en relación con los casos que implican a más de un estado miembro.

Esta tutela administrativa del derecho a la protección de datos personales no excluye sino que cede ante la protección penal de los datos personales cuando se ha cometido alguno de los delitos previstos en el Código Penal (CP).

A pesar del breve repaso a los conceptos básicos y principios, es preciso advertir que existen normas específicas para determinadas bases de datos (operadores de telecomunicación, ADN, policiales, etc.), que recogen conceptos y principios particulares en relación con la materia tratada.

4. Normativa europea: presente y futuro

I. Los orígenes del derecho a la protección de datos

El derecho fundamental a la protección de datos de carácter personal es uno de los llamados derechos de tercera generación. Con la irrupción de las nuevas ideas de la Ilustración, a finales del S. XVIII y principios del S. XIX surgen los derechos fundamentales de corte clásico: El derecho a la vida, la libertad, la igualdad, y la seguridad, entre otros. La segunda generación de derechos fundamentales sur-

gen con el llamado Estado del bienestar, de esta forma nacen nuevos derechos fundamentales, entre los que cabe destacar: Derecho de asociación, de sindicación, al trabajo digno y a la huelga, derecho a la salud física y mental, a la Seguridad Social y a la educación obligatoria.

Por último, en la segunda mitad del S. XX, después de la segunda guerra mundial, surgen una nueva generación de derechos fundamentales, algunos autores como PÉREZ LUÑO[1] los denominan la *tercera generación de derechos humanos,* entre los que se destacan: a la paz y coexistencia pacífica, los derechos de los consumidores, el derecho a la calidad de vida y el disfrute del medio ambiente, y la libertad informática.

La protección de los datos personales se ubica dentro del nuevo derecho fundamental a la denominada libertad informática o buen uso de las ciencias y la tecnología, aunque está surgiendo un nuevo movimiento que defiende la plasmación legal de una cuarta generación de derechos fundamentales como garantías del ciudadano ante el mal uso de la informática y las redes de comunicación.

La preocupación social por la protección de datos personales surge en los países desarrollados a principios de los años 70, aunque, como luego se comprobará, su primera plasmación legislativa se produce en Europa, por lo tanto, estamos ante un derecho eminentemente europeo y surgido en nuestro continente.

En Estados Unidos, la primera llamada de atención[2], por la que se subraya la necesidad de proteger la intimidad frente a la irrupción de las nuevas tecnologías tiene unos antecedentes bien definidos, que en el plano doctrinal lo encontramos ya en 1969 con ALAN F. WESTIN, autor fundamental en la materia, quien publica un artículo titulado «*Computers and the protection of privacy*», en donde se evidencia los peligros que para la intimidad puede acarrear la, entonces incipiente, era de las computadoras y la necesidad de que el Derecho diese una respuesta para proteger la intimidad de las personas frente a los posibles ataques que pudieran producirse.

Pero lo que desencadenó en Estados Unidos la necesidad de una normativa al respecto fue el llamado caso Watergate, que obligó a dimitir al entonces presidente Nixon, donde quedó patente que el

[1] PÉREZ LUÑO, Antonio-Enrique, «*Intimidad y Protección de Datos Personales del Habeas Corpus al Habeas Data*», en el colectivo «Estudios sobre el Derecho a la Intimidad», p. 37.

[2] TÉLLEZ AGUILERA, Abel, «*La protección de datos en la Unión Europea: Divergencias normativas y anhelos unificadores*», p. 22 y ss.

poder podía fácilmente sucumbir a la tentación de utilizar las nuevas tecnologías para irrumpir en la intimidad de cualquiera.

Este interés por la protección a la intimidad provocó que el 31 de diciembre de 1974 se promulgase la «*Privacy Act*», en cuya exposición de motivos se dice: «*El Congreso estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información por entes y órganos federales...el creciente uso de los ordenadores y de una tecnología compleja de la información, si bien es esencial para el eficiente funcionamiento de las Administraciones Publicas, ha aumentado de forma importante el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal*».

En Europa, la sensibilidad hacia la protección de los datos personales surge con cierta antelación al continente americano, como ejemplo la Comisión Consultiva surgida en 1967 en el seno del Consejo de Europa con la finalidad de estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, particularmente sobre el derecho a la intimidad, aunque «*la intimidad*» como tal ya había sido recogida en varios documentos internacionales, por ejemplo, la Declaración Universal de los Derechos Humanos ya reconocía la necesidad de proteger el derecho a la intimidad de la persona en su art. 12, el art. 8 del Convenio para la Protección de los Derechos Humanos de las Libertades Fundamentales, realizado en Roma el 14 de noviembre de 1950, o en el art. 17.1 del Pacto Internacional de los Derechos Civiles y Políticos de Nueva York de 19 de diciembre de 1966.

El trabajo de la citada Comisión Consultiva para estudiar las tecnologías de la información y su potencial peligro hacia los derechos de las personas, desencadenó en la Resolución n.º 509 de la Asamblea del Consejo de Europa sobre «*Los derechos humanos y los nuevos logros científicos y técnicos*».

A partir de este momento, en Europa comienzan a surgir las primeras normas nacionales sobre la materia, la primera ley de protección de datos, que como tal aparece en Europa, es la promulgada en Alemania por el Land de Hesse el 7 de octubre de 1970, para continuar el 11 de mayo de 1973 la promulgada por el parlamento sueco, que entró en vigor el 1 de julio de ese mismo año.

El 20 de noviembre de 1973, el Consejo de Europa promulga su Resolución 22/1973 sobre regulación jurídica de los ficheros electrónicos en el sector privado y, un año más tarde, el 29 de noviembre de 1974 la Resolución 29/1974 se ocupa de establecer normas regu-

ladoras del sector público de la informática. La mayoría de los autores, entre otros DAVARA RODRÍGUEZ y TÉLLEZ AGUILERA[3], estiman que estas resoluciones son la verdadera génesis del movimiento legislativo que recorrerá Europa en materia de protección de datos.

II. Desarrollo europeo de la protección de datos y situación presente

De manera paralela a las normativas nacionales, el Consejo de Europa[4] desarrolló una serie de estándares para la protección de los datos personales a través del Convenio 108 para la protección de los individuos con respecto al tratamiento automatizado de sus datos personales, adoptado en Estrasburgo el 28 de enero de 1981 y que entró en vigor el 1 de octubre de 1985.

Este fue el segundo instrumento internacional sobre la materia que apareció en pocos meses, ya que en septiembre de 1980 la Organización para la Cooperación y el Desarrollo Económico (OCDE) también había adoptado sus «Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales».

El Convenio 108 estuvo seguido unos años después por la Directiva 95/46/CE de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de datos. Además, surgen normas más específicas en materia de protección de datos, cabe destacar la Directiva 2002/58/CE relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[5].

El citado Convenio tiene un mayor ámbito de aplicación que la Directiva, pues ésta sólo se aplica a los datos personales procesados en el desarrollo de actividades que tradicionalmente han estado reguladas por la normativa comunitaria, mientras que el Convenio no está sujeto a esta limitación y se aplica con carácter general a todo procesamiento de datos personales llevado a cabo en el ámbito de cualquier actividad, si bien los Estados pueden limitar su ámbito de aplicación.

---

[3] DAVARA RODRÍGUEZ, Miguel Ángel, «*La protección de datos en Europa*», p. 30; TÉLLEZ AGUILERA, Abel, «*La protección de datos en la Unión Europea: Divergencias normativas y anhelos unificadores*», p. 29.

[4] SUTTON, Graham: «*El Consejo de Europa*», en la obra colectiva «*Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*», p. 63 y ss.

[5] Consecuencia de dicha normativa europea, se promulga en España la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y redes públicas de comunicaciones.

El Convenio 108 establece las principales normas que aún inspiran las legislaciones europeas en materia de protección de datos personales, a continuación se exponen brevemente los principios más importantes:

1. En el art. 1 se garantiza el respeto de los derechos y libertades de cualquier persona física, sea cual fuere su nacionalidad o residencia, concretamente su derecho a la vida privada, con respeto al tratamiento automatizado de los datos de carácter personal correspondientes a cada persona.

   Por lo tanto se aplica a todos los ciudadanos que se encuentren en territorio europeo y que la protección de datos es un derecho íntimamente ligado a la privacidad.

2. El ámbito del Convenio se extiende al tratamiento automatizado de datos personales del individuo, en virtud de la Directiva 95/46/CE todos los Estados también deben aplicar sus normas sobre protección de datos a ciertas categorías de ficheros manuales y algunos Estados han elegido extender su protección a las personas jurídicas.

3. El art. 5 se refiere a la calidad de los datos y a la necesidad de que sean obtenidos legal y legítimamente, que deben ser almacenados para finalidades concretas y legítimas, y no ser usados para fines que puedan ser incompatibles con dicha finalidad inicial.

   Los datos deben ser adecuados, relevantes y no excesivos. Deben ser precisos y actualizados cuando sean necesarios.

   Por último, los datos deben ser conservados de manera que permitan la identificación del sujeto afectado por un tiempo no superior al necesario para cumplir la finalidad para la cual han sido recogidos.

4. Según el art. 6, existen diversas categorías de datos que son enumerados en el citado precepto, algunos especialmente sensibles que requieren unas garantías apropiadas, aunque no sugiere o específica la naturaleza concreta de tales garantías.

5. El art. 7 requiere la adopción de medidas de seguridad adecuadas contra riesgos de seguridad específicos. A este respecto el Informe de 2002 del Consejo de Europa sobre «*El impacto de los principios sobre protección de datos relativos al proceso penal en el ámbito jurídico de la cooperación judicial penal*» muestra su preocupación sobre el creciente riesgo para la vida privada que representan las nuevas tecnologías, especialmente

cuando las sentencias penales aparecen publicadas en los medios de comunicación o en otros medios como Internet.

6. El art. 7 establece el derecho de cualquier persona a conocer si el responsable del tratamiento está procesando sus datos personales y, en tal caso, a obtener información específica de dicho tratamiento. Una manera de cumplir con esta obligación es a través del registro de información que los responsables del tratamiento están llamados a notificar a las autoridades supervisoras en materia de protección de datos.

   El Convenio 108 no exige un sistema de notificación o registro, esta obligación surge como novedad en la Directiva 95/46/CE, aunque ya era recogido en muchos países que adoptaron sus legislaciones sobre protección de datos antes de la Directiva y se había introducido dicho mecanismo.

7. El art. 7 también establece el derecho de acceso a la información, es decir, poder acceder a los datos personales que son objeto de tratamiento

8. El art. 8 regula el derecho del sujeto afectado por el tratamiento a recurrir si sus derechos han sido infringidos y en el art. 10 obliga a los Estados a establecer un sistema efectivo de sanciones y recursos en casos de infracción de las normas sobre protección de datos.

El Convenio tiene dos importantes carencias, la necesidad de establecer autoridades independientes sobre la materia y las restricciones que han de establecerse cuando la información se refiere a terceros Estados. Ambas limitaciones han sido reguladas posteriormente a través del Protocolo Adicional al citado Convenio 108 de 1 de julio de 2004, actualmente ratificado por 30 países.

Además de la citada normativa Comunitaria, debemos destacar los instrumentos surgidos a raíz de los tratados de la Unión Europea, siendo los más importantes[6]:

I. La protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea:

La Carta de Derechos Fundamentales de la Unión Europea tiene la virtud de establecer, en un único documento, un conjunto de

[6] Siguiendo el desarrollo efectuado por GUTIÉRREZ ZARZA, Ángeles, «*Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea*» y «*El tratado de Funcionamiento de la Unión Europea*», en la obra colectiva «*Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*», p. 63 y ss.

derechos para todos los ciudadanos europeos y para todas aquellas personas que se encuentren y residan en la Unión Europea.

Los derechos regulados se dividen en seis secciones, la segunda se dedica a las libertades y, a este respecto, contienen dos preceptos importantes:

> Art. 7. «*Respeto de la vida privada y familiar: Todos tienen derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.*»
>
> Art. 8. «*Protección de datos de carácter personal:*
>
> 1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
> 2. *Estos datos se tratarán de modo legal, para fines concretos y sobre la base del consentimiento de la persona afectada y en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
> 3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*»

Esta Carta fue firmada y proclamada por los presidentes del Parlamento Europeo, de la Comisión y del Consejo Europeo el 7 de diciembre del año 2000 en Niza, y refleja los principios generales reconocidos anteriormente por la Convención Europea de Derechos Humanos de 1950, actualizados por la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de las Comunidades Europea.

Según el art. 51 de la Carta de Derechos Fundamentales, se aplica a las instituciones, los órganos, las oficinas y las agencias de la Unión Europea y, por tanto, sus actos (legislativos y no legislativos) deben estar de acuerdo con ella.

De acuerdo con el art. 52 de la misma Carta, los derechos y libertades reconocidos en la misma, sólo podrán limitarse respetando el principio de proporcionalidad y siempre que tales limitaciones sean necesarias y respondan a objetivos de interés general reconocidos por la Unión, o ante la necesidad de protección de los derechos y libertades de los demás.

II. El Tratado de Funcionamiento de la Unión Europea.

La entrada en vigor del Tratado de Lisboa el 1 de Diciembre de 2009 introdujo dos novedades fundamentales en materia de protección de datos:

1.º La Carta de Derechos Fundamentales de la Unión Europea recibe el mismo carácter vinculante que los Tratados, tal y

como se declara expresamente en el art. 6 del Tratado de la Unión, recordemos que el Artículo 8 reconoce el derecho a la protección de datos el carácter de derecho fundamental.

2.º El Tratado de Funcionamiento de la Unión Europea, regula la materia de protección de datos con carácter general, sin hacer distinción entre las materias de derecho civil y mercantil (antes reguladas por la Directiva 95/46/CE) y las propias de derecho penal (antes excluidas de la citada Directiva).

Con la entrada en vigor del Tratado de la Unión Europea, la Carta de Derechos Fundamentales de la Unión Europea recibe el mismo carácter vinculante que los tratados, tal y como se declara expresamente en el art. 6 del Tratado de la Unión.

El citado art. 8 de la Carta ha sido reproducido literalmente en el art. 16 del Tratado de Funcionamiento de la Unión Europea, de esta manera se refuerza la necesidad de respetar el derecho fundamental a la protección de datos en la Unión Europea.

Art. 16.

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

2. El Parlamento Europeo y el consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el art. 39 del Tratado de la Unión Europea.»

El Tratado de Lisboa introdujo sin embargo dos matices importantes al citado Artículo 16 TFEU:

El primero, la posibilidad de excluir del ámbito general de protección de datos las materias de orden público y seguridad del Estado. El art. 39 del Tratado de la Unión Europea y aplicable en el ámbito de la Política Exterior y de Seguridad Común, dispone:

Art. 39. «*De conformidad con el art. 16 del Tratado de Funcionamiento de la Unión Europea y, no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las activi-*

dades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

El segundo matiz, la Declaración n.º 21 aneja al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, firmado en diciembre de 2007. La Declaración n.º 21, sobre la protección de datos personales en el ámbito de la cooperación judicial y policial en material penal que dispone:

«*La Conferencia reconoce que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el art. 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos.*»

Esta Declaración junto con el citado art. 16.2 del Tratado de Funcionamiento de la Unión Europea motivó el debate sobre la conveniencia de incluir, en la nueva normativa que debería reemplazar a la Directiva 95/46/CE, normas específicas sobre el tratamiento y la protección de datos personales para fines policiales y judiciales.

En materia criminal, cabe destacar el Convenio sobre Ciberdelincuencia, realizado el 23 de noviembre de 2001 en Budapest, con instrumento de ratificación de mayo de 2010, que conmina a la adopción de medidas para tipificar como delito cualquier acceso deliberado e ilegítimo a un sistema informático con la intención de obtener datos informáticos.

III. Futuro sobre la regulación europea en materia de protección de datos

El 25 de enero de 2012, la Comisión Europea[7] presentó un paquete de medidas para la reforma del régimen de protección de datos personales, con la finalidad de reforzar la protección del derecho a la privacidad en línea, reforzar la confianza de los consumidores en los servicios *on line* y promover el crecimiento, la creación de empleo y la innovación europea.

El nuevo paquete de medidas incluye una Comunicación de la Comisión, una propuesta de Reglamento sobre protección y libre

[7] *Vid.* Gutiérrez Zarza, Ángeles, *op. cit.,* pp. 100 y ss.

circulación de datos personales y una propuesta de Directiva sobre protección y tratamiento de datos personales por las autoridades policiales y judiciales.

La propuesta del nuevo Reglamento pretende poner al día y revisar los principios y derechos reconocidos en la Directiva 95/46/CE para adaptarse a los cambios que exige la nueva era digital. Se introducen nuevos principios como:

— Transparencia: Los responsables del tratamiento deben informar a los ciudadanos con toda transparencia para que sepan quién recoge y trata los datos.

— Reforzar el principio de minimización de los datos, es decir, la recogida de los datos debe limitarse al mínimo necesario en relación a los fines de que se trate.

— Obligación de informar sobre infracciones en materia de seguridad.

— Aumentar las categorías de datos sensibles.

— Precisar el tipo de consentimiento que debe otorgarse en determinados casos, especialmente en un entorno digital.

También se contemplan nuevos derechos, a destacar:

— La «portabilidad de los datos» que permitirá al ciudadano retirar sus datos, listado de amigos y cualquier otro detalle personal de una aplicación o servicio informático y transferirlos a otra aplicación o servicio distinto, incluyendo la información almacenada en la llamada «nube». La portabilidad de los datos se regula en el art. 18 de la propuesta de reglamento.

— El «derecho al olvido» que otorgará a los ciudadanos el derecho a que sus datos personales no sean tratados más allá del tiempo en el que son necesarios o por más tiempo del plazo máximo legal previsto, salvo que se solicite expresamente la autorización del individuo al cual se refiere. Este derecho se regula en el art. 17 de la propuesta de Reglamento. Pretende evitar que nuestros datos figuren eternamente en los buscadores de internet, por ejemplo la notificación de una multa en un Boletín Oficial.

— Se pretende aumentar el control de los individuos sobre sus propios datos personales y asegurar el ejercicio de los derechos de acceso, rectificación, borrado o bloqueo de los datos personales, especialmente en las redes sociales *on line*. Es de-

cir, se pretende impedir que los individuos no sean capaces de retirar fotos de servidores de internet, o que puedan crearse registros de usuarios cuando los internautas visitan sitios web mediante uso de las *cookies* o instrumentos similares.

— El art. 8 de la propuesta de Reglamento regula el tratamiento de los datos personales relativos a los niños y dispone que, en el caso de menores de 13 años, el tratamiento sólo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño.

— También se prevén mecanismos de recurso colectivo para permitir a grupos de ciudadanos y algunas entidades cualificadas reclamar mediante el ejercicio conjunto de acciones de reclamación de daños en supuestos de vulneración del derecho a la protección de datos.

Por último, también se pretende realizar modificaciones en cuanto a los procedimientos, principalmente la reducción de las cargas administrativas a los responsables del tratamiento como suprimir la obligación del responsable del tratamiento de notificar a las autoridades de protección de datos todas las operaciones de tratamiento de datos.

Actualmente, estas propuestas son objeto de debate en el Parlamento Europeo con fuertes presiones de los *lobbys* que representan a las grandes empresas de Internet. Las modificaciones obligarán a modificar nuestra legislación nacional para su adecuación a la normativa Europea.

5. Normativa española

En los apartados anteriores, se ha puesto de manifiesto que la protección de datos personales es un derecho fundamental dotado por la mayor protección en el ámbito europeo y que debe ser regulado por las normativas nacionales de acuerdo con los parámetros marcados en Europa.

I. La Constitución Española y la jurisprudencia del Tribunal Constitucional

Es preciso subrayar que, con antelación a muchos de las normas europeas antes citadas, la Constitución Española de 1978 ya con-

templa esta protección dentro de los derechos fundamentales que regulan el derecho a la intimidad:

Art. 18.4 «*La ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*»

Es cierto reconocer que, de la lectura del precepto, no puede extraerse como conclusión que los constituyentes estuvieran identificando la naturaleza y contenido del bien que trataban de proteger.

La jurisprudencia del Tribunal Constitucional[8] no ha sido ajena a la dificultad de desentrañar el bien jurídico protegido que justifica su regulación como derecho fundamental y, a tal efecto, surgen una serie de sentencias que ponen de manifiesto la evolución doctrinal al respecto.

La primera sentencia dictada al efecto es la STC 254/1993, de 20 de julio, en la que el alto tribunal afirma que el art. 18.4 de la C. E. (Fundamento Jurídico 6), «*... una garantía constitucional para responder a una nueva amenaza...*», especificando seguidamente al señalar que, «*además de un instituto de garantía de otros derechos, fundamentalmente el honor y a la intimidad, es también, en si mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos*».

Por lo tanto, ya se reconoce que el contenido del citado precepto constitucional descansa sobre la base de un nuevo derecho fundamental e instrumental para la protección de otros derechos y libertades.

Posteriormente se producen otras sentencias, siendo preciso destacar las STC 11/1998, de 13 de abril, por ser la primera que introduce el término «*privacidad*» en el ámbito de la protección de datos y como un concepto distinto al de intimidad, siendo el primero un término que abarca un ámbito más amplio que el de la intimidad. También destacable es la STC 202/1999, de 8 de noviembre, donde siguiendo la línea de las anteriormente mencionadas en la que se entiende vulnerado el derecho del recurrente a la intimidad, pero sin concretar totalmente un derecho autónomo e independiente a pesar de emplear el término «*libertad informática*» (Fundamentos Jurídicos 2.º y 5.º).

---

[8] Prieto Gutiérrez, Jesús, «*La Jurisdicción Constitucional ante la Protección de Datos Personales*», pp. 5 y ss. Boletín de Información del Ministerio de Justicia de 1 de noviembre de 2000.

Las primeras sentencias que realmente definen un derecho fundamental autónomo e independiente son las SSTC 290 y 292/2000, ambas de 30 de noviembre, en ambas sentencias, y concretamente en la sentencia en la 292, el Tribunal Constitucional viene a concretar el alcance del derecho fundamental a la protección de datos de carácter personal con la finalidad de garantizar el poder de control de los individuos respecto de sus datos personales, así como sobre el uso y destino de los mismos.

El Tribunal[9] deja sentada la importancia del derecho a la protección de datos, calificándolo como un derecho independiente, autónomo, diferenciado del derecho a la intimidad y que transciende al uso de la informática. Es un derecho que va mucho más allá de la intimidad y que tiene un enganche directo con los diversos textos internacionales del más alto rango (fundamento jurídico 8.º de la sentencia 292).

II. La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

La ratificación del Convenio 108 por España, el 27 de enero de 1984, hacía necesaria la aprobación de una ley de protección de datos y así se hizo mediante Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal que, además venía a desarrollar el art. 18.4 de la Constitución Española.

Esta primera norma sobre la materia llegó tarde, cuando ya entonces se discutía en la entonces Comunidad Económica Europea una nueva norma más amplia, así surge la Directiva 95/46/CE que obliga a los países miembros a legislar en materia sobre protección de datos siguiendo una serie de parámetros.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), transpone la Directiva al ordenamiento interno español, y hoy día constituye el marco legislativo esencial por el que se regula el derecho a la protección de datos personales en nuestro país, aunque también debe tenerse en cuenta las leyes que algunas Comunidades Autónomas han aprobado sobre la materia, dentro del marco previsto en el art. 41 de la LOPD, por

[9] Piñar Mañas, José Luis, «*La protección de datos personales y ficheros automatizados*», en el colectivo «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales*», p. 155.

ejemplo la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal de la Comunidad de Madrid.

La LOPD deroga la LO 5/1992, sirviendo como marco legal aplicable con carácter general[10] a cualquier tratamiento de datos que se lleve a cabo por entidades privadas o por particulares, como por entidades públicas.

En esta norma se desarrolla el contenido del derecho y se establecen los principios que conforman el mismo, de acuerdo con lo establecido en el marco normativo europeo, con dos importantes precisiones, solo se aplica a datos de personas físicas sometidos a tratamiento, sea éste automatizado o no automatizado. Por tanto, los datos de personas jurídicas no gozan del régimen de garantías que la misma dispensa, y tampoco los de las personas físicas no sujetas a tratamiento.

La LOPD contiene 49 artículos, 6 disposiciones adicionales, 3 disposiciones transitorias, 3 disposiciones finales y 1 disposición derogatoria, una circunstancia curiosa es que no contiene exposición de motivos.

En los arts. 4 a 12 (Título II), se recogen los principios de la protección de datos: calidad de los datos, derecho de información de los interesados, consentimiento del afectado, protección especial de determinados datos, el encargado del tratamiento debe adoptar medidas de seguridad para proteger los datos almacenados, el deber de secreto al responsable de fichero y a quienes intervengan en él, sólo se puede comunicar los datos a un tercero para el cumplimiento de determinados fines y el acceso a los datos por cuenta de tercero.

Los arts. 13 a 20 (Título III), regula los derechos específicos de las personas a destacar: el derecho de acceso a sus datos personales que son objeto de tratamiento, el derecho de rectificación y cancelación, la tutela de los derechos por la Agencia de Protección de Datos y el derecho a ser indemnizado como consecuencia del incumplimiento de lo dispuesto de la LOPD.

La LOPD garantiza lo que constituye el núcleo duro básico del derecho fundamental a la protección de los datos personales y transpone al ordenamiento interno el contenido de la Directiva 95/46/CE, aunque la ley no acaba de eliminar la excesiva cantidad de conceptos jurídicos

[10] Piñar Mañas, José Luis, «*Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal*», Boletín del Ilustre Colegio de Abogados de Madrid. La protección de datos (I), núm. 35 febrero 2007, pp. 19 y ss.

indeterminados[11] que la Directiva lógicamente maneja para facilitar una transposición que aproxime las diversas legislaciones internas.

La LOPD es una normativa escueta que necesita de un reglamento para su desarrollo, de esta forma surge el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la LOPD 15/1999, de 13 de diciembre (BOE de 19 de enero de 2008). Muy importante para poder analizar, entender y aplicar los derechos y principios contenidos en la Ley.

Antes de entrar a la exposición de la normativa penal, conviene analizar las infracciones y sanciones administrativas contenidas en la LOPD para diferenciar la potestad sancionadora de la Agencia Española de Protección de Datos de los ilícitos penales que serán de aplicación de forma supletoria de acuerdo con el principio de intervención mínima que rige en el Derecho penal (principio de subsidiariedad o *ultima ratio* y el carácter fragmentario).

En los arts. 43 y ss. (Título VII) de la LOPD, se recogen las infracciones y sanciones que se pueden imponer a los responsables de los ficheros y los encargados de los tratamientos. Las infracciones pueden ser calificadas como leves, graves o muy graves.

Las leves son infracciones menores en la forma de llevar los ficheros o por no respetar debidamente los derechos del afectado, como por ejemplo: no atender la solicitud del interesado de rectificación o cancelación, no proporcionar la información solicitada por la Agencia de Protección de datos (cuando no sean aspectos sustantivos de la protección), recoger datos de carácter personal sin proporcionar la información adecuada a los interesados, etc.

Las infracciones graves se refieren a quebrantos importantes de los principios y derechos contenidos en la LOPD, como puede ser: Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal sin autorización, proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos con finalidades distinta de las que constituyen el objetivo legítimo de la empresa, proceder a la recogida de datos sin el consentimiento expreso de las personas afectadas cuando éste sea exigible, mantener datos inexactos o no efectuar las rectificaciones o cancelaciones de los mismos, mantener los ficheros sin las condiciones de seguridad, etc.

[11] García Meseguer, María Dolores y Medrán Vioque, Rafael, «*La protección de las personas físicas en el tratamiento de datos: Principios y Derechos. Breve Comentario de la Transposición de la Directiva 95/46/CE a la Ley Orgánica 15/1999*», Boletín de Información del Ministerio de Justicia de 15 de junio de 2002, Boletín 1919, p. 18.

Por último, las infracciones muy graves son el último escalón anterior al delito y son las siguientes:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidos.

c) Recabar y tratar los datos que hagan referencia al origen racial, a la salud y a la vida sexual, cuando no medie consentimiento expreso del afectado o una ley que lo habilite. Violentar la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual de las personas.

d) No cesar en el uso ilegítimo de los tratamientos de datos cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de los datos con destino a países que no proporcionen un nivel de protección equiparable sin autorización de la Agencia de Protección de Datos.

f) Tratar los datos de una forma ilegítima o con menosprecio de los principios y garantías que le sean de aplicación.

g) La vulneración de guardar secreto sobre los datos de carácter personal especialmente protegidos, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

En muchas situaciones será difícil deslindar el ilícito administrativo del penal.

6. Regulación penal en España

El Código penal de 1995 (CP) es el primer Código español que incorpora una rúbrica específica para que la «intimidad» figure como bien jurídico protegido, de esta forma el Título X del Libro II lleva por título «*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*».

Anteriormente, sólo el art. 497 bis del CP de 1973 hacía referencia a la «intimidad» introducido tras la reforma operada por LO 7/1984, de 15 de octubre, pero en ningún caso se hace mención a la protección de los datos personales.

Por lo tanto, el art. 197.2 del CP, introduce por primera vez la sanción penal por las conductas ilícitas sobre los datos de carácter personal o familiar.

> Art. 197.2 «*Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*»

I. Bien jurídico protegido

Por la ubicación sistemática del precepto, el bien jurídico protegido podría parecer que es la intimidad, pero el epígrafe anterior se ha podido comprobar que, desde la STC 290/2000, de 30 de noviembre, el Tribunal Constitucional desgaja la protección de los datos personales de la noción de intimidad y los califica como derechos fundamentales independientes, aunque su estrecha relación es innegable. Es más, pienso que legislador del 1995 cuando introdujo el precepto en el CP no estaba pensando en un bien jurídico protegido independiente, tal es así que la Jurisprudencia del TC hasta esa fecha no le reconocía tal categoría.

Para ROMERO CASABONA[12] el bien jurídico protegido son los datos reservados de carácter personal o familiar de otro, para ALONSO DE ESCAMILLA[13] en este apartado del art. 197 se regula el tipo base de los delitos contra la libertad informática o «*habeas data*». En realidad son dos posturas complementarias, como pone de manifiesto la Jurisprudencia del Tribunal Supremo.

---

[12] ROMEO CASABONA, Carlos María, «*Los datos de carácter personal como bienes jurídicos penalmente protegidos*», en el colectivo «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales*», pp. 186 y 187

[13] ALONSO DE ESCAMILLA, Avelina, «*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*», en el colectivo «*Delitos y faltas. La parte especial del derecho penal*», pp. 218 y 219.

La STS 1328/2009, de 30 de diciembre de 2009 (La Ley 273457/2009), en su fundamento jurídico 6.º indica:

> «*Consecuentemente, como ya hemos indicado, lo que se protege en este apartado segundo es la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido.*»

II. Aspecto objetivo

Sujetos: En principio, el sujeto activo de delito puede ser cualquier persona, salvo la encargada o responsable de los ficheros porque integraría el subtipo agravado del apartado 5.º

> Art. 197.5.º «*Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.*»

Si el sujeto activo es funcionario público puede integrar el subtipo agravado del art. 198.

La conducta típica debe realizarse por el sujeto activo «*sin estar autorizado*» para llevarla a cabo, como por ejemplo, el acceso indebido a la fuente de datos reservados de carácter personal o familiar, registrados en ficheros de la Seguridad Social (STS 725/2004, de 11 de junio de 2004, La Ley 1787/2004). Es una característica del tipo formulada negativamente y, en el supuesto de concurrir la autorización para apoderarse, utilizar, modificar o acceder a los datos reservados registrados, la conducta será atípica, sin perjuicio de que el acto pueda ser sancionado por la vía administrativa.

El sujeto pasivo es el titular de los datos reservados de carácter personal o familiar registrados en archivos o ficheros. El titular de los datos nunca puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su privacidad. Conducta típica: La modalidad básica incluye tres figuras diversas: La primera hace referencia al apoderamiento, utilización o modificación, a este respecto la STS 1328/2009:

> «*"Se apodere" se ha interpretado por un sector doctrinal en sentido estricto como el apoderamiento que precisan los delitos contra el patrimonio. Otro sector se inclina por una interpretación más amplia comprendiendo los supuestos en que se copian los datos, dejando intactos*

los originales o simplemente se capta, se aprehende, el contenido de la información, acepción en la que "apoderase" resultaría equivalente a acceder al dato que se castiga también en el inciso final. "Utilizar" es usar sin apoderarse de ellos. "Modificar" es alterar los mismos, tanto si trata de mejorar como de perjudicar la situación del sujeto al que afectan.»

En segundo lugar el precepto se refiere al verbo acceder, es decir, tener acceso a los datos, captarlos o tomar conocimiento de los mismos.

Por último, al final de precepto también se vuelve hacer referencia al verbo utilizar, es decir, usar sin apoderamiento, y del verbo alterar que puede considerarse sinónimo de modificar.

Se aprecia una deficiente técnica legislativa en el empleo de verbos para describir la conducta típica, con una reiteración y solapamiento respecto de las acciones típicas del primer inciso (utilizar y modificar) y el tercer inciso (utilizar y alterar). Objeto material del delito: El art. 197.2 CP nos remite a los datos reservados de carácter personal o familiar, de esta forma la STS 725/2004, de 11 de junio de 2004 (La Ley 1787/2004), en su fundamento jurídico 2.º indica:

«*Sin embargo, el tipo del art. 197.2 CP no hace distinciones respecto del objeto de la acción que tengan fundamento en normas no penales y se refiere a "datos reservados de carácter personal o familiar" registrados en soportes informáticos, electrónicos o telemáticos de archivos o registros públicos o privados. Es decir, que el legislador ha querido alcanzar todos los datos de estas características porque, indudablemente, todos son merecedores de protección penal.*»

Según el fundamento jurídico 6.º de la STS 1328/2009:

«*Los datos, además, han de estar recogidos (registrados) en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier tipo de archivo o registro público o privado... En el sentido del art. 197.2 debe exigirse que se trate de un conjunto organizado de información relativa a una generalidad de personas. Dado el carácter reservado de los datos, los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades específicas, siendo indiferente, su naturaleza: personal, académica o laboral, médica, económica, etc. Se trata, en realidad de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad.*»

La citada sentencia indica que las conductas debe ir dirigidas a datos que se hallen registrados, es decir, deben operar sobre ficheros o bancos de datos preexistentes, y entiende que no es típica la creación clandestina de bancos de datos, debiendo castigarse dicha conducta en el ámbito administrativo. En este sentido la sentencia

de 11 de junio de 2010, de la Sección 6.º de la Audiencia Provincial de Madrid (SAP de Madrid 281/2010 Sección 6.ª La Ley 67019/2010) absuelve a los imputados por la cesión de datos contenidos en un listado que no reúne los requisitos del tipo.

Los datos o información deben pertenecer al ámbito privado y personal o familiar del sujeto, de este modo el fundamento de derecho 3.º de la STS 1461/2001, de 11 de julio (La Ley 6768/2001) recuerda que, aunque en el artículo se refiere a datos reservados de carácter personal o familiar, no siendo preciso que pertenezcan al núcleo duro de la privacidad, pues de ser así se aplicaría la agravación del apartado 5.º del art. 197, si es necesario que afecten a la intimidad personal. Posteriormente la STS 1328/2009, de 30 de diciembre, indica:

> «*Hay que distinguir entre la irrelevancia "objetiva" del contenido e importancia de la información para que la protección penal opere en el caso de datos de carácter personal o familiar, a que se refiere el art. 197.2, que, desde el punto de vista sustancial y aisladamente considerados, son generalmente inocuos; y la necesaria equiparación que debe establecerse entre "secreto" y "reservado" a efectos de la intimidad personal y familiar. En efecto de una interpretación teleológica y sistemática se debe concluir que el término reservado que utiliza el Código hay que entenderlo como "secretos" y "no público", parificándose de este modo el concepto con el art. 197.1 CP. Secreto será lo desconocido u oculto, refiriéndose a todo conocimiento reservado que el sujeto activo no conozca o no esté seguro de conocer y que el sujeto pasivo no desea que se conozca.*»

De esta forma la sentencia citada absuelve al acusado porque el único dato que obtuvo con un uso inadecuado del programa informático de consulta clínica, fue el relativo al nombre del médico de cabecera del también médico del mismo centro, no accediendo a ningún otro dato de su historia clínica, y el dato del médico de cabecera no es un dato que el hombre medio de nuestra cultura considera «*sensible*» o «*reservado*». Dicha conducta debe ser sancionada en el ámbito administrativo pero no está reviste carácter penal.

La Sentencia de la Audiencia Provincial de Navarra, de 20 de septiembre de 2011 (SAP de Navarra 154/2011 de la Sección 1.ª La Ley 291265/2011), absuelve a un médico de empresa que accedió a la historia clínica que constaba en atención primaria, de la que también era médico, accediendo sin autorización a su expediente y a los datos personales, pero no consta que accediese a datos diferentes que no constasen ya en el expediente obrante en el servicio médico de empresa, por lo que no concurre el requisito de que los datos sensibles fueren reservados o secretos con la persona del acusado.

III. Aspecto subjetivo

La conducta del tipo básico de los delitos con la libertad informática sólo admite la comisión dolosa, excluyéndose su incriminación imprudente de acuerdo con lo previsto en el art. 12 CP.

Además, el artículo exige que el sujeto activo actúe «en perjuicio de tercero». Se trata de otra manifestación de la deficiente técnica legislativa que se percibe en la confusión provocada por el requisito de «obrar en perjuicio de tercero» cuando se trata de apoderase, utilizar o modificar datos, de no exigir perjuicio alguno cuando se solamente se acceda y por, último, de exigir nuevamente en el inciso final «en perjuicio del titular de los datos o de un tercero» cuando se trata alterar o utilizar datos.

Aquí el Tribunal Supremo se ha tenido que emplear a fondo para realizar una interpretación racional y sensata al respecto. A propósito de este tema, la cuestión ya comienza a ser analizada en la STS de 18 de febrero de 1999, en la misma se llega a la conclusión de que no debía conceptuarse la expresión «en perjuicio de tercero» como un ánimo específico de perjudicar (elemento subjetivo del injusto), cuya ausencia convertiría en impunes conductas que había puesto al descubierto la intimidad de otro, atacando abiertamente el «*habeas data*». De no entenderlo así quedaría desprotegido el bien jurídico que se trata de tutelar, haciendo ilusoria la previsión punitiva. La sentencia indicada concluye que nos hallamos ante un delito doloso, pero no de tendencia.

Pero en la STS 1461/2001, de 11 de julio de 2001 (La Ley 6768/2001), en su fundamento jurídico 3.º analiza de una forma pormenorizada la cuestión planteada, tomando como punto de partida la anterior sentencia:

> *«Pero el problema sigue en pie, a pesar de la interpretación ensayada por la mentada sentencia de 1999.*
>
> *La pregunta es la siguiente: la expresión "en perjuicio de tercero", ¿debe interpretarse como un plus, en la lesión del bien jurídico? Esta Sala entiende que existen argumentos para responder negativamente al interrogante:»*

Los argumentos se pueden resumir en los siguientes:

a) Si el ámbito de la intimidad protegida se restringe mucho, se produce el efecto de asimilar el perjuicio a la parte más básica de la intimidad, lo que se conoce como núcleo duro de la privacidad (salud, ideología, vida sexual, creencias religio-

sas, etnia o raza,..), pero ese perjuicio ya se castiga como un subtipo agravado en el núm. 6 del art. 197, lo que conlleva la inaplicación en el art. 197.2 CP.

b) La conducta se consuma sin necesidad de que un ulterior perjuicio se produzca, se consuma tan pronto el sujeto activo accede a los datos, los conoce, los tiene a su disposición, con ello quebranta la reserva que los cubre.

c) El precepto trata de poner freno a los abusos informáticos contra la intimidad, es decir, contra aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento queda reservado a su titular.

De esta forma la STS 1461/2001, de 11 de julio de 2001, concluye:

> «*Trasladando tales consideraciones al caso enjuiciado, es incontestable que el sujeto o activo del delito desveló unos datos, secretos o reservados, a los que no tenía acceso, poniendo al descubierto aspectos personales del sujeto afectado, sin su consentimiento y con el daño consiguiente de su derecho a mantenerlos ocultos (intimidad), lo que integra "el perjuicio" exigido. En el término "tercero" debe incluirse al afectado en su intimidad, sujeto pasivo, que es al que esencialmente se refiere el tipo.*»

La STS 1328/2009, de 30 de diciembre, en su fundamento jurídico 10.º tomando como punto de partida las dos sentencias anteriores, especialmente la primera, tiene que realizar una nueva interpretación del precepto, a fin de entender que todas las conductas descritas exigen el requisito del perjuicio, incluso cuando se refiere al verbo «acceso», que en principio no exige tal expresión.

> «*Pues bien, creemos que es necesario realizar una interpretación integradora en el sentido de que como en el inciso primero, se castigan idénticos comportamientos objetivos que en el inciso 2.º (apodere, utilice, modifique) no tendría sentido de que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles –y con la misma pena– en el inciso segundo.*»

Además, en dicha sentencia se una hace una nueva interpretación del concepto de perjuicio, entendiendo que cuando se ponen al descubierto datos sensibles, aquellos que ponen al descubierto aspectos personales del afectado, su apoderamiento o divulgación ya comportan el daño exigido, pero si no trata de ese tipo de datos debe probarse el perjuicio ocasionado.

> «*Y en cuanto a la distinción entre datos "sensibles" y los que no lo son, debe hacerse en el sentido de que los primeros son por sí mismos ca-*

paces para producir el perjuicio típico, por lo que el acceso a los mismos, su apoderamiento o divulgación, poniéndolos al descubierto comporta ya ese daño a su derecho a mantenerlos secretos u ocultos (intimidad) integrando el "perjuicio" exigido, mientras que en los datos "no sensibles", no es que no tenga virtualidad lesiva suficiente para provocar o producir el perjuicio, sino que debería acreditarse su efectiva concurrencia y en el caso presente, no se ha acreditado –ni se ha articulado prueba en ese sentido– de que el acceso por parte del recurrente al nombre del médico cabecera –dato administrativo, y en principio, inocuo– del Dr. Bienvenido haya ocasionado perjuicio a éste como titular del dato».

IV. Subtipos agravados

En el anterior apartado, se han puesto de manifiesto algunos subtipos agravados, concretamente aquellos que hacen referencia al sujeto activo, uno de ellos previsto en el apartado 5.º que hace referencia a la mayor penalidad cuando la acción típica es llevada a cabo por los encargados de los ficheros o responsables de los soportes informáticos que serán castigados con penas de 3 a 5 años, el segundo de ellos previsto en el art. 198 CP que castiga con la pena en su mitad superior del tipo básico más inhabilitación absoluta de 6 a 12 años, cuando se cometa por autoridad o funcionario público.

Ambos son supuestos de un delito especial impropio y que, en el primer caso, se justifica en la quiebra del deber de custodia y sigilo que se presupone a las personas encargadas de los ficheros. En el segundo supuesto, se quebranta la confianza depositada por la sociedad en las autoridades o funcionarios públicos.

En el art. 197.4.º se castiga con pena de 2 a 5 años, la difusión, revelación o cesión de datos a terceros, siendo la pena de 1 a 3 años y multa de 12 a 24 meses cuando quien lo divulga no ha tomado parte en su descubrimiento.

El fundamento de esta cualificación radica en la mayor intensidad del ataque al bien jurídico protegido, y la modalidad se consuma cuando la información reservada se pone en conocimiento de terceros.

El art. 197.6.º se regula un subtipo agravado por la afectación a datos personales especialmente sensibles o protegidos, de acuerdo con el art. 7 de la LOPD, o que afecten a menores de edad o incapaces. Se imponen las penas del tipo básico en su mitad superior.

En el art. 197.7.º también castiga con las penas en su mitad superior cuando los hechos tienen una finalidad lucrativa, es decir, existe un elemento subjetivo equivalente al ánimo de lucro de los delitos

patrimoniales que se produce cuando el autor desea obtener un beneficio económico, ganancia o utilidad evaluable económicamente.

Y, por último, el art. 197.8.º también castiga con la pena superior en grado cuando los hechos se producen en el seno de una organización o grupo criminal.

V. Casuística

A continuación, se analizaran algunos supuestos prácticos para la mejor comprensión del ilícito penal estudiado:

1. El médico del centro de salud no está autorizado para acceder a la historia clínica de las personas que no son pacientes suyos (SAP de Navarra 20 de septiembre de 2011, La Ley 291265/2011)
2. Los funcionarios del INEM no están legitimados para acceder a las bases de datos de la seguridad social y apropiarse de datos que no deberían conocer por razón de su cargo (STS 11 de junio de 2004, La Ley 1787/2004).
3. El acceso indebido a una cuenta de correo electrónico e incluso su utilización para enviar un correo, conlleva el uso y el acceso a datos reservados de carácter personal de aquellos a los se refiere el art. 197.2, mediante la indebida introducción en esa cuenta de correo y su utilización mediante el envío de un correo electrónico. (SAP de Navarra de 10 de marzo de 2009, La Ley 96197/2009).
4. Para vulnerar la intimidad de su víctima, accedió a su correo electrónico y se apoderó de archivos en los que se contenía fotografías de ella, las cuales modificó, apoderándose de datos reservados de carácter personal, y utilizándolos además en la forma que se ha descrito en esta resolución (SAP de Valladolid de 4 de abril de 2011, La Ley 61574/2011).
5. Estamos ante la presencia de actos de apoderamiento de un correo electrónico y de un acceso a un fichero o soporte informático como es el listado de correo electrónico de la Sra. Dolores, la comprobación del tráfico por ésta sostenido y la selección de unos concretos mensajes por ésta mantenidos (SAP de Barcelona de 18 de enero de 2008, La Ley 7257/2008).
6. Una empresa que contrata a un trabajador temporal de una ETT para la prestación de un servicio consistente en la ac-

tualización de la base de datos de sus pacientes de la clínica, posteriormente crea una página web (imitando la de la empresa) en la que publica los datos de los pacientes (código, nombre y apellidos). El trabajador no es condenado por un delito del art. 197.2 CP, sino por un delito de descubrimiento de secretos de empresa (SAP de Sevilla de 19 de octubre de 2007, La Ley 279757/2007).

7. Los datos del lugar de trabajo y el domicilio de la empresa están tan protegidos como los demás, y por lo tanto se trata de un acceso indebido a datos protegidos. (STS 11 de junio de 2004, La Ley 1787/2004).
8. Cuando un médico accede a una historia clínica de forma indebida y no obtiene dato alguno que difiera de los que ya tenía conocimiento en su labor profesional, no comete el delito el art. 197.2 por cuanto no accede a datos reservados o secretos, con independencia de lo inadecuado o indebido de los citados accesos a la historia clínica que deben ser sancionados en la vía administrativa. (SAP de Navarra de 20 de septiembre de 2011, La Ley 291265/2011).
9. Un jefe de negociado utiliza las claves de una auxiliar administrativa para acceder a las hojas del padrón municipal, obtenido 40 hojas con los datos personales y familiares que allí constan y cuyo destino se ignora. El acusado obtiene datos personales con quebranto del bien jurídico protegido y haciéndolo por cauces no autorizados (STS 11 de julio de 2001, La Ley 6768/2001).
10. El único dato que el acusado obtuvo con el uso inadecuado del programa informático de consulta clínica, fue el relativo al nombre del médico de cabecera del también médico del mismo centro, no estando acreditado que accediera a cualquier otro dato, y el dato del médico de cabecera no es un dato que el hombre medio de nuestra cultura considera sensible por ser inherente al ámbito de su intimidad. Consecuentemente la cuestión no reviste carácter penal (STS 30 de diciembre de 2009, La Ley 273457/2009).

7. La regulación en el proceso penal español

La parte del ordenamiento jurídico que lleva más retraso en la regulación de la protección de datos es el derecho procesal, a pesar de

que resulta difícil imaginar un proceso penal donde no sea necesario aportar información que se encuentra en bases de datos.

La identificación de la persona detenida (huellas dactilares, fotografías), la comprobación de sus antecedentes delictivos y penales, los registros de voz, perfiles de ADN, propietarios de vehículos, visionado de cámaras de seguridad, etc. Existen multitud de información obrante en ficheros y bases de datos que son necesarios para la investigación penal.

Dentro de los derechos fundamentales, ya hemos visto que la persona física es titular del derecho fundamental a la protección de datos personales, incluso algún autor como GUTIERREZ ZARZA[14] defiende que este derecho fundamental le asiste al imputado en un proceso penal, aunque hasta la fecha no haya sido objeto de protección en el ámbito procesal.

La realidad es que la Ley de Enjuiciamiento Criminal de 1882 no regula en precepto alguno el acceso a bases de datos y la incorporación esta información al proceso. Una norma tan antigua no puede regular una realidad que era inexistente en aquella época, por tanto se hace necesario una nueva regulación que responda a la problemática actual.

El Proyecto de Ley de Enjuiciamiento Criminal que llegó al parlamento en la anterior legislatura regulaba, en su Título VIII, los medios de investigación relativos a datos protegidos, de esta forma en su Capítulo I con la rúbrica «El acceso y tratamiento de datos personales», se regulaba el acceso a datos personales contenidos en ficheros (art. 415), la necesaria autorización del Juez de Garantías para acceder a las historias clínicas (art. 416), la búsqueda selectiva y cruce datos previa autorización del Juez de Garantías. Asimismo en los arts. 419 y ss., se regulaba la conservación de datos relativos a comunicaciones electrónicas y la autorización judicial sobre datos de tráfico y contenido relativo a comunicaciones.

Como es sabido, el anteproyecto no llegó a tramitarse por la finalización de la legislatura y al comienzo de la presente, el actual

---

[14] GUTIÉRREZ ZARZA, Ángeles, «*La protección de datos personales como derecho fundamental del imputado ¿también en el ámbito del proceso penal?*, La Ley Penal, mayo 2010, «*Según la jurisprudencia existente hasta el momento, el derecho a la protección de datos personales asiste también al sujeto imputado en un proceso penal pero, la posible vulneración de este derecho fundamental se hace valer, en la mayoría de las ocasiones, ante la correspondiente agencia de protección de datos... Es de esperar que en un futuro próximo las líneas que separan y los lazos que unen la protección de datos y el proceso penal pueda apreciarse claramente...*».

Gobierno ha vuelto a presentar el 25 de febrero de 2013 un nuevo anteproyecto de Código Procesal Penal.

En el mismo se dedica el Libro IV al Proceso Ordinario, con un Título II que regula el contenido de las diligencias de investigación y cuyo Capítulo XII se refiere a la «Incorporación de datos personales automatizados al proceso», y más concretamente indica:

> Art. 353. «*Disposición general. El Ministerio Fiscal podrá requerir a cualquier persona física o jurídica responsable del fichero automatizado la cesión de aquellos datos personales que sean relevantes para el esclarecimiento del hecho investigado o la identificación de su autor.*
>
> Art. 354. «*Cruce y contraste de datos personales. Cuando la investigación del hecho, atendidas las exigencias impuestas por los principios, idoneidad, necesidad y proporcionalidad, exija el cruce, comparación y contraste entre datos personales que obren en archivos automatizados de cualquier persona física o jurídica, el Fiscal podrá autorizar la medida por decreto, que será impugnable ante el Tribunal de Garantías*».
>
> Art. 355. «*Excepciones. 1. Si los datos se hallaran incorporados a un ordenador, sistema o dispositivo de almacenamiento masivo utilizado por el encausado, el acceso a los mismos se ajustará a lo previsto en el art. 349* (autorización judicial para el registro de dispositivos de almacenamiento masivo de información). *2. La cesión de datos contenidos en la historia clínica del encausado o de un tercero requerirá, en todo caso, autorización judicial. 3. La cesión de datos especiales generados como consecuencia de las comunicaciones electrónicas o telemáticas se regirá por lo dispuesto en el art. 312 de este Código (*acceso a los datos necesarios para la identificación del usuario y del terminal).

Pero la nueva norma regula otros aspectos sobre la recogida de datos procedentes de ficheros, cabe destacar:

Art. 310. Incorporación al proceso de datos electrónicos obrantes en archivos automatizados de los operadores de servicio.

Art. 311 y 312. Acceso a los datos necesarios para la identificación del usuario y del terminal, mediante la IP, o numeración IMSI o IME.

Art. 330. Captación de imágenes en espacios públicos.

Art. 331. Utilización de dispositivos técnicos de seguimiento y localización.

Art. 347 a 349. Registro de dispositivos de almacenamiento masivo de información.

Art. 350 a 352. Registros remotos sobre equipos informáticos.

En cuanto al reconocimiento e identificación del encausado, también se regula la identificación fotográfica (art. 277), el reconocimiento de voces (art. 278) y la investigación mediante ADN (arts. 287 a 290).

Como se puede apreciar, la nueva normativa trata de adecuarse a la Jurisprudencia del Tribunal Supremo, Tribunal Constitucional y Tribunal Europeo de Derechos Humanos que, en los últimos años, ha intentado llenar las lagunas normativas respecto a los métodos de investigación que proporcionan las nuevas tecnologías.

8. Conclusiones

De la exposición anterior, se puede vislumbrar que todavía nos encontramos en una etapa muy incipiente de la regulación de la protección de los datos personales, el principal motivo radica en que se trata de un derecho de reciente aparición y, por tanto, todavía no se encuentra delimitado y estructurado de una forma nítida y clara. A pesar de este punto, las Instituciones Europeas desean incrementar la protección a este derecho fundamental porque se han dado cuenta de los peligros que encierran el uso inadecuado de las nuevas tecnologías.

A continuación vamos a poner un ejemplo de cómo la recogida e intercambio de nuestros datos personales pueden permitir, a terceras personas, tener un conocimiento completo de lo que hacemos, cómo vivimos, cómo pensamos.

Veamos un ejemplo: Si vamos a pasar unos días de vacaciones a Nueva York, los datos que damos a la compañía aérea (PNR, passenger name record) son retenidos para gestionar el viaje, pero después serán enviados las autoridades americanas que realizarán «ciertas comprobaciones» a los efectos de prevención y detención de actividades delictivas.

Si nuestro destino turístico anterior ha sido algún país árabe o africano (Mali, Libano, Israel), Estados Unidos realizará comprobaciones adicionales y pedirá explicaciones a la llegada al aeropuerto.

Si realizamos alguna transferencia bancaria desde un lado a otro del océano, nuestra transferencia será enviada por la compañía *swift* a las autoridades americanas, quienes comprobaran con todo detalle quien es el destinatario de nuestro dinero, todo ello con la justificación de evitar que se financien actividades terroristas o se propaguen los delitos.

Los perfiles de ADN y las huellas dactilares de personas con antecedentes penales son chequeados de manera automática, cada noche, con perfiles y huellas similares almacenados en los otros Estados miembros de la Unión Europea que participan en el sistema Prüm.

Las compañías telefónicas tienen la obligación de retener durante un periodo de tiempo que oscila entre los 6 meses y los 2 años, los datos de tráfico de nuestras conversaciones.

El convenio sobre Cibercrimen establece un nuevo marco normativo para interceptar, de manera remota y en tiempo real, toda la información almacenada en un ordenador o en los correos electrónicos que se envían o reciben.

Fuera del ámbito penal, los nuevos sistemas inteligentes de control de energía doméstica almacenan datos sobre la hora que salimos o llegamos casa, cuando nos vamos a dormir o nos levantamos, si estamos en una misma habitación la mayoría de la tarde o nos ubicamos en otras estancias.

La introducción de esta ponencia comienza hablando de Orwell, evocando su obra «1984», pero es que la sociedad orwelliana ya está aquí, ya se ha introducido en nuestras vidas de una forma evidente. Todavía estamos a tiempo de marcar un territorio de protección que permita al individuo escapar a ese control absoluto perseguido por las nuevas tecnologías, aunque existan fuerzas muy poderosas que intentarán rebasar dichos límites por múltiples razones, principalmente la seguridad como en la obra de Orwell.

Bibliografía citada

ALONSO DE ESCAMILLA, Avelina: «*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*», en el colectivo»*Delitos y faltas. La parte especial del derecho penal*», Colex, Madrid, 2012.

DAVARA RODRÍGUEZ, Miguel Angel, «*La protección de datos en Europa*»; Madrid, 1998.

GARCÍA MESEGUER, María Dolores y MEDRÁN VIOQUE, Rafael, «*La protección de las personas físicas en el tratamiento de datos: Principios y Derechos. Breve Comentario de la Transposición de la Directiva 95/46/CE a la Ley Orgánica 15/1999*», Boletín de Información del Ministerio de Justicia de 15 de junio de 2002, Boletín 1919.

GUTIÉRREZ ZARZA, Ángeles, «*Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea*» y «*El tratado de Funcionamiento de la Unión Europea*», en la obra colectiva «*Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*». La Ley, Las Rozas (Madrid), 2012

– «*La protección de datos personales como derecho fundamental del imputado ¿también en el ámbito del proceso penal?*, La Ley Penal, mayo 2010.

PÉREZ LUÑO, Antonio-Enrique, «*Intimidad y Protección de Datos Personales del Habeas Corpus al Habeas Data*», en el colectivo «Estudios sobre el Derecho a la Intimidad», Tecnos, Madrid, 1992.

PIÑAR MAÑAS, José Luis, «*La protección de datos personales y ficheros automatizados»,* en el colectivo «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales*», Comares, 2006

– «*Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal*», Boletín del Ilustre Colegio de Abogados de Madrid. La protección de datos (I), núm. 35 febrero 2007.

PRIETO GUTIÉRREZ, Jesús, «*La Jurisdicción Constitucional ante la Protección de Datos Personales*», pp. 5 y ss. Boletín de Información del Ministerio de Justicia de 1 de noviembre de 2000.

ROMEO CASABONA, Carlos María, «*Los datos de carácter personal como bienes jurídicos penalmente protegidos*», en el colectivo «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales*». Comares, Granada, 2006.

SUTTON, Graham: «*El Consejo de Europa*», en la obra colectiva «*Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*». La Ley, Las Rozas (Madrid), 2012.

TÉLLEZ AGUILERA, Abel, «*La protección de datos en la Unión Europea: Divergencias normativas y anhelos unificadores*». Edisofer S. L., Madrid, 2002.