Ana Isabel Herrán Ortiz

El derecho a la protección de datos personales en la sociedad de la información

Derechos humanos

Universidad de Deusto

Instituto de Derechos Humanos

Cuadernos Deusto de Derechos Humanos

Cuadernos Deusto de Derechos Humanos

Núm. 26

El derecho a la protección de datos personales en la sociedad de la información

Ana Isabel Herrán Ortiz

Bilbao
Universidad de Deusto
2003

Publicación impresa en papel ecológico

Apartado 1 - 48080 Bilbao

ISBN: 978-84-9830-576-0

Indice

I. **Intimidad y protección de datos personales. Formulación jurídica del concepto de privacidad**

1. *El derecho a la intimidad. Su significado como derecho de la persona*

Ha sido una necesidad constante en el ámbito jurídico ofrecer una definición de lo que deba entenderse por intimidad, y delimitar su configuración como bien jurídico. Ello no obstante, y como quiera que resulta imposible formular una definición exhaustiva del concepto intimidad, se propone un estudio de su contenido esencial y sus diversas manifestaciones, así como de su naturaleza jurídica como derecho de la persona.

1.1. Naturaleza jurídica del derecho a la intimidad

El concepto y la idea de intimidad encuentran en el ámbito jurídico su fundamento y significado en el principio de la «dignidad de la persona» y de la tutela de la personalidad individual[1]; y en verdad, que el derecho a la intimidad constituye una manifestación de la dignidad humana, y así se desprende de la propia definición que el TC propone cuando afirma que «la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respecto por parte de los demás» (STC 53/1985). En efecto, la definición de los ámbitos de reserva de la persona y el control de los mismos constituye una manifestación del derecho a la libertad individual, cada persona ha de decidir la medida en la que desea ser dejado en paz y mantener en su esfera privada datos personales.

Lo cierto es que la dignidad de la persona garantiza el pleno desarrollo de la personalidad individual, al tiempo que, por un lado, implica el reconocimiento de la plena autodisposición, sin injerencias externas, de las posibilidades de actuación propias de cada persona; y por otro lado, conlleva la autodeterminación que nace de la libre proyección humana, y que se encuentra vinculada a la idea de intimidad

[1] Así, ha declarado el TC que «Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 CE, aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la "dignidad de la persona", que reconoce el art. 10 de la CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana» (Cfr. STC 231/1998).

personal y familiar[2]. La caracterización del derecho a la intimidad como derecho de la persona se encuentra unida a la identificación de su función jurídica y al contenido esencial que el ordenamiento jurídico le atribuye.

Así, en principio puede decirse que el derecho a la intimidad es un derecho de la personalidad porque constituye un bien instrumental para garantizar la libertad del individuo en el desarrollo de su propia vida. Luego, la libertad individual se erige en fundamento necesario de la dignidad humana, y el derecho a la intimidad se configura como elemento esencial para el desarrollo de la personalidad. Asimismo, si los derechos de la personalidad se definen como bienes que garantizan el disfrute por cada persona de sus propias facultades físicas, intelectuales y morales, y sin los cuales el ser humano quedaría desprovisto de sus principales garantías para asegurar su pleno y efectivo desarrollo, habrá que concluir también que el derecho a la intimidad destaca entre los derechos de la personalidad[3].

Ciertamente, los derechos fundamentales en general, y el derecho a la intimidad en particular, contribuyen a establecer y mantener las condiciones mínimas para el desarrollo de la libertad y la dignidad de la persona. Asimismo, el derecho a la intimidad se caracteriza como derecho fundamental por su configuración como derecho subjetivo de defensa y de protección positiva o libertad para sus titulares[4]. En efecto, se ha superado la tradicional concepción del derecho a la intimidad

---

[2] Así se manifiesta Pérez-Luño, A.E., *Derechos humanos, Estado de Derecho y Constitución,* Tecnos, Madrid, 1986, p. 318.

[3] Recordar las afirmaciones del TC, por las que: «[…] Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la CE aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad… Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo». Cfr. STC 231/1988, de 2 de diciembre, BOE núm. 307, 23 de diciembre de 1988.

[4] En este sentido, advierte el TC que «La protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones Públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. […] Al desconocer estas facultades, y no responder a las peticiones deducidas, la Administración del Estado hizo impracticable el ejercicio de su derecho a la intimidad, dificultando su protección más allá de lo razonable, y por ende vulneró el art. 18 de la Constitución». Cfr. STC 254/93, de 20 de julio, BOE núm. 197, 18 de agosto de 1993.

como derecho a ser dejado en paz, para acoger en su ámbito una esfera de protección positiva, que se manifiesta en el reconocimiento de determinadas facultades para exigir y facilitar un ámbito de libertad y el pleno ejercicio de los derechos de las personas; en definitiva, se aspira a garantizar el control de la información que nos concierne y que otros conocen de nosotros, no se trata de reaccionar cuando nuestra intimidad se ha visto vulnerada, sino de exigir positivamente del Estado deberes de tutela del derecho, y en todo caso, de garantizar facultades para la tutela y defensa de las libertades de la persona[5]. No hay que olvidar, por otra parte, que los derechos fundamentales y, entre ellos, el derecho a la intimidad, sustentan un concreto sistema de valores y principios en un contexto cultural y social determinado, legitimador del orden jurídico y constitucional.

1.2. Revisión conceptual del derecho a la intimidad

Han sido numerosos los intentos por ofrecer una definición del derecho a la intimidad, y todos ellos han coincidido en establecer una vinculación directa entre este bien jurídico y la esfera más próxima e interior de la persona. Ciertamente, el derecho a la intimidad contempla al individuo desde su perspectiva más interior, desde la esencia que lo define y diferencia de los demás. En consecuencia, el derecho a la intimidad se define como un derecho de la persona a decidir por sí mismo en qué medida desea compartir con otros sus pensamientos, sus sentimientos y su vida personal. Luego, el bien jurídico tutelado por el derecho a la intimidad se corresponde con el modo de ser de la persona, sustraído al conocimiento ajeno, porque su revelación le ocasionaría una perturbación en su dignidad como ser humano, y mermaría su desarrollo individual.

De todo ello se concluye que el derecho a la intimidad constituye una respuesta jurídica a las aspiraciones de cada persona por alcanzar un ámbito de desarrollo interior, ajeno a la intromisión de terceros. Ahora bien, el derecho a la intimidad no debe identificarse erróneamente con el derecho de exclusión de terceros del ámbito privado de cada persona,

---

[5] Como bien ha declarado Rebollo Delgado el reconocimiento del derecho a la intimidad no se reduce a la posibilidad o no de los titulares de ejercitar las correspondientes acciones judiciales cuando se ha producido una violación de los mismos, sino que además los poderes públicos han de adoptar las medidas necesarias para proteger al ciudadano de los ataques de terceros contra la intimidad, para que su ejercicio sea real y efectivo. Rebollo Delgado, Lucrecio, *El derecho fundamental a la intimidad*, Madrid, Dykinson, 2000, p. 78.

antes bien, al contrario, representa el derecho a controlar y decidir sobre la información y la vida privada que sólo a cada uno concierne. Por tanto, el derecho a la intimidad asegura una calidad mínima de vida en las relaciones con los terceros, de suerte que únicamente se conozca aquello que cada persona desea compartir y revelar a los demás, bien entendido que en ningún caso por ello se pierde el control sobre la propia información personal.

En este sentido, resultan de especial valor las afirmaciones de FARIÑAS MATONI, diferencia el autor un derecho objetivo, como reconocimiento que el ordenamiento jurídico dispensa al derecho a la intimidad, y un derecho subjetivo a la intimidad, entendido como facultad del hombre, esgrimible erga omnes, consistente en poder graduar la relación con el exterior, y que comporta la posibilidad de solicitar el pertinente amparo del ordenamiento jurídico cuando dicha facultad sea transgredida[6].

En efecto, no puede negarse que el hombre es un ser social por naturaleza, llamado a relacionarse con los demás, pero es precisamente esa necesidad natural la que le impulsa a mantener y conservar una vida interior, ajena a las relaciones exteriores que le unen con otros individuos. En definitiva, el derecho a la intimidad no se asienta sobre la ocultación de determinados aspectos de la personalidad del individuo al conocimiento ajeno, sino sobre la necesidad de un ámbito de libertad interior, como instrumento imprescindible para el pleno desarrollo de la personalidad individual y como garantía de respeto a la dignidad personal[7].

2. *El derecho fundamental a la protección de datos. De las dificultades para su configuración jurídica*

No ha sido cuestión pacífica la necesidad y oportunidad jurídica del reconocimiento de un nuevo derecho fundamental a la protección de datos personales. En efecto, fueron frecuentes e intensos los debates que enfrentaron a la doctrina a propósito de la configuración del derecho a la protección de datos, si bien es cierto que en la actualidad las recientes afirmaciones del TC, estableciendo el reconocimiento de un nuevo derecho fundamental a la protección de datos, han venido a clarificar una cuestión que había sido tan controvertida.

---

[6] FARIÑAS MATONI, Luis M.ª, *El derecho a la intimidad,* Trivium*,* Madrid, 1983, p. 352.

[7] HERRÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999, p. 11-12.

2.1. El origen del derecho a la protección de datos. Las Generaciones de Derechos Fundamentales

El reconocimiento de que el catálogo de los derechos humanos sea permeable y abierto a la incorporación de nuevos valores no ha sido un principio unánimemente admitido por la doctrina, claro que los avances tecnológicos han reclamado del legislador respuestas a las nuevas pretensiones individuales derivadas de los importantes cambios sociales que aquellos fenómenos introducen. En verdad, el progreso social y el desarrollo tecnológico demandan no sólo protección en la más estricta intimidad del individuo, sino también garantías para asegurar el gobierno de la persona en sus relaciones con terceros.

Por todo ello, junto a los tradicionales derechos fundamentales, se reconoce el ejercicio de otros, que defienden al individuo en su dimensión social, y que alcanzan significación cuando se tutela a la persona en su condición de ser social. Se trata de derechos de los que se disfruta plenamente cuando la persona se relaciona con su entorno, y le aseguran un bienestar en su vivir cotidiano en sociedad. Así, se han definido tres «generaciones» de derechos fundamentales, cada una de ellas se corresponde con un concreto momento histórico y cultural, que facilitó el reconocimiento y aparición de derechos fundamentales marcados por las circunstancias ideológicas y políticas que acontecían en cada momento histórico.

La Primera Generación de Derechos Fundamentales, se caracterizaba por derechos de naturaleza individualista, y de defensa; con su ejercicio se aspiraba a garantizar al individuo la no intromisión por los poderes públicos en la esfera personal de cada ciudadano. Sin embargo, de forma temprana, se pone de manifiesto la necesidad de incorporar nuevos derechos fundamentales, que aseguren la participación y actuación de los ciudadanos en la vida pública, surge entonces la Segunda Generación de Derechos Fundamentales, los llamados derechos sociales, económicos y culturales. Nace con ellos la obligación para los poderes públicos de desarrollar actividades que aseguren el cumplimiento de tales derechos, y así, sólo se reconocerá efectiva protección a los ciudadanos cuando se garanticen positivamente por los poderes públicos las condiciones para que tales derechos sean reales y efectivos.

En la actualidad, el imparable desarrollo social, y en concreto, el avance de la sociedad de la información, exigen respuestas jurídicas precisas, adecuadas a los nuevos fenómenos sociales que la vida moderna ofrece a las personas. Aparece de este modo, con el impulso de los nuevos avances sociales y tecnológicos, la Tercera Generación de Derechos Fundamentales, son los llamados derechos de la solidaridad, que superan el ámbito individual y se refieren a cuestiones de interés

general. Son derechos tales como la protección del medio ambiente, la tutela de derechos de consumidores y usuarios o la protección de la persona frente a la irrupción tecnológica.

Centrado el derecho a la protección de datos en un momento histórico y social concreto son numerosas las cuestiones que sobre su configuración jurídica quedan aún sin respuesta, a saber: ¿Cuál es el origen inmediato del derecho a la privacidad o protección de datos? ¿Goza de naturaleza jurídica propia? ¿Ha de reconocerse su condición de derecho fundamental?

Hay que situar su origen en la célebre sentencia del Tribunal Constitucional alemán de 1983, que por vez primera acuña la expresión «autodeterminación informativa» y establece una definición de la naturaleza y contenido de este nuevo derecho. En efecto, reconoce el TC alemán que el derecho a la protección de datos ha de enmarcarse en el derecho general de protección de la persona, por considerar que garantiza la facultad del individuo a determinar por sí mismo la divulgación y utilización de datos referentes a su persona, y alerta asimismo del peligro que representa para los derechos de la persona un nuevo fenómeno unido a la irrupción de la informática, «el enmallamiento» de la información[8]; porque son infinitas las posibilidades que la informática ofrece en el tratamiento de datos personales, permitiendo no sólo una recogida sin límites en el tiempo o el espacio, sino también y, lo que tal vez sea más grave, facilitando el entrecruzamiento de los datos, y su cesión a terceros, que sin duda escapa al conocimiento y disposición de la persona. Abundando en lo expresado, coincidimos con el TC alemán cuando previene que lo decisivo en la protección de datos no es la naturaleza íntima o no del dato cuyo registro se pretende, lo verdaderamente relevante será la utilización, la finalidad del tratamiento o la posible interconexión de los datos personales tratados[9].

---

[8] En palabras del TC alemán «En virtud de esta evolución de los condicionamientos tecnológicos, es posible producir una imagen total y pormenorizada de la persona respectiva —un perfil de la personalidad— incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal"». Traducción de Daranas Peláez, Manuel, «Jurisprudencia constitucional Extranjera. Tribunal Constitucional Alemán. Ley del Censo», *Boletín de Jurisprudencia Constitucional,* núm. 33, 1984, p. 137.

[9] «Un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia, y en esa medida ya no existe, bajo las condiciones de elaboración automática de datos, ningún dato "sin interés". El grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad. Hace falta más bien conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho a la personalidad». Traducción de Daranas Peláez, Manuel, «Jurisprudencia constitucional Extranjera. Tribunal Constitucional Alemán. Ley del Censo», *art. cit.,* p. 155.

Así las cosas, lo cierto es que también pueden encontrarse importantes manifestaciones del reconocimiento jurisprudencial de este nuevo derecho en el Derecho español, y así el TC español pronto abrió las puertas a la configuración de un nuevo derecho o al menos a la necesidad de una revisión del concepto tradicional del derecho a la intimidad[10].

Por todo ello, la protección de datos personales constituye una respuesta jurídica frente al fenómeno de la sociedad de la información, para frenar la potencial amenaza que el desarrollo tecnológico representa para los derechos y libertades de las personas. Ahora bien, se encontraba enfrentada la doctrina a propósito del reconocimiento y origen de un nuevo derecho fundamental a la protección de datos; y así, no han faltado autores que rechazando la consideración del derecho a la protección de datos como derecho fundamental, apostaban por una reformulación del tradicional derecho a la intimidad como garantía individual ante el avance informático[11]. Por nuestra parte, consideramos, sin embargo, que constituye una necesidad incontestable el reconocimiento de un nuevo derecho fundamental a la protección de datos personales, cuya construcción jurídica reposaría sobre la atribución y reconocimiento a la persona de un haz de facultades de disposición respecto a la información que le concierne, y que supera el contenido esencial del tradicional derecho a la intimidad[12].

2.1. El derecho a la protección de datos y su categorización jurídica

Antes de iniciar el análisis del contenido y naturaleza del derecho a la autodeterminación informativa conviene recordar la decisiva contribución

---

[10] «Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y el respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida». Cfr. STC 110/84, de 26 de noviembre, BOE núm. 305, de 21 de diciembre de 1984.

[11] Es de esta opinión Ortí Vallejo, Antonio, *Derecho a la intimidad e informática, Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada,* Comares, Granada, 1994, pp. 31 y ss.

[12] Coincidimos, por tanto, con las consideraciones expresadas por Lucas Murillo de la Cueva, Pablo, «Informática y protección de datos personales. Estudios sobre la Ley Orgánica 5/92, de regulación del tratamiento automatizado de los datos de carácter personal», *Cuadernos y Debates,* núm. 43, CEC, Madrid, 1993, pp. 33 y ss.

del Tribunal Constitucional a la configuración jurídica de la protección de datos personales en el Derecho español, ya que a través de la célebre STC 254/93 se determinaron los principios jurídicos sobre los que se asienta la construcción legal y jurisprudencial del derecho a la protección de datos personales. En efecto, a este pronunciamiento judicial se debe el acierto de afirmar que la relación de derechos fundamentales no es una lista cerrada, y que todos los derechos fundamentales en última instancia constituyen instrumentos jurídicos para la tutela de la dignidad humana, y en concreto, que el art. 18.4 CE incorpora una nueva garantía constitucional[13].

2.1.1. Como derecho de la personalidad

Una aproximación al bien jurídico tutelado a través del derecho a la protección de datos permite concluir que el fundamento último de este derecho no consiste exclusivamente en preservar oculta información relativa a la vida privada, sino en garantizar el pleno desarrollo de la personalidad individual y el libre ejercicio de sus derechos; se trata en definitiva de impedir la instrumentalización del ser humano, que debe manifestarse en la sociedad con plena libertad. Por ello, resulta consecuencia necesaria la configuración del derecho a la protección de datos como derecho de la personalidad. Siendo esto así, lo cierto es que el individuo demanda protección por el tratamiento de sus datos personales no sólo frente a los poderes públicos, sino también frente a la actuación de los particulares. El Gran Hermano de Orwell no debe identificarse exclusivamente con la Administración pública, las empresas privadas disponen en la actualidad de sistemas informáticos capaces de competir con el sector público. Por tanto, puede decirse que el derecho a la protección de datos aspira a garantizar a la persona el disfrute y respeto a su propia identidad e integridad en todas las manifestaciones físicas y espirituales, y es precisamente su fundamento último el que permite afirmar su condición de derecho de la personalidad.

Recapitulando, se puede proclamar que el derecho a la protección de datos es un derecho de la personalidad por su condición de derecho inherente a la persona; esto es, el bien jurídico tutelado es propio de la persona, y necesario para el pleno desenvolvimiento de su personalidad, en tanto que su vulneración priva a la persona del disfrute y goce de los más significativos derechos y libertades.

---

[13] Cfr. STC 254/93, de 20 de julio, BOE núm. 197, de 18 de agosto de 1993.

2.1.2. Como derecho fundamental

¿La proclamación constitucional contenida en el artículo 18.4 constituye una base suficiente para afirmar el origen de un nuevo derecho fundamental a la protección de datos? ¿Es posible, por otra parte, reformular el concepto de intimidad y adecuarlo a las exigencias de la sociedad de la información sin que la protección de la persona se debilite?

Estas cuestiones enfrentaron a la doctrina a propósito del reconocimiento de un nuevo derecho fundamental a la protección de datos; bien es verdad que en la actualidad el Tribunal Constitucional ha ofrecido respuesta a tan polémica cuestión, al afirmar que el artículo 18.4 de la CE «no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona… pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos propicie comportamientos discriminatorios» (STC 11/98, de 13 de enero).

La necesidad y conveniencia del reconocimiento de un derecho fundamental a la protección de datos se encuentra apoyado sobre la base de tres principios esenciales: primero, los debates parlamentarios en torno al artículo 18.4 de la CE avalan la importancia y significación de esta proclamación constitucional; segundo, la tradicional concepción preinformática del derecho a la intimidad no ofrece respuesta eficaz a la exigencia de tutela de la persona en la sociedad informática y tercero, la especial naturaleza y significación de los bienes jurídicos implicados en el desarrollo de las nuevas formas de comunicación hace necesario configurar formas de respuesta adecuadas a estos nuevos fenómenos tecnológicos.

A propósito de la incidencia de los debates parlamentarios previos a la aprobación del texto constitucional, fueron intensas y enfrentadas las opiniones de los diferentes Grupos Parlamentarios respecto al alcance y la oportunidad del artículo 18.4 de la CE[14]. En este sentido, se

[14] A este respecto se advertía «parece que estamos hablando de una técnica más (en alusión a la informática), pero es una técnica cada vez con más incidencia en el ámbito de estos derechos individuales a que nos estamos refiriendo. Es evidente, que existe una tendencia objetiva hacia la utilización creciente de la informática, penetrando en el dominio de lo que debe ser estrictamente la esfera de la privacidad, de la independencia y de la libertad del ciudadano. Consideramos, por tanto, muy útil que en la Constitución se hable sobre este tema y justamente en este precepto». Cfr. Diario de sesiones del Congreso de los Diputados. Comisión de Asuntos Constitucionales y Libertades Públicas, núm. 70, 19 de mayo de 1978, p. 2528.

muestran especialmente reveladoras las afirmaciones defendidas por el Grupo Minoría Catalana, que ya entonces alertaban sobre el peligro y las infinitas posibilidades que la informática ofrecía para condicionar y afectar el desarrollo de los derechos y libertades de las personas, se destacó la importancia de un precepto llamado a limitar el uso de la tecnología para tutelar el ejercicio eficaz de los derechos de los ciudadanos[15]. En la actualidad, se ha evidenciado la especial significación del art. 18.4 CE, que permite constitucionalizar la defensa de todos y cada uno de los derechos de los ciudadanos frente al uso indiscriminado de los medios informáticos; esto es, en palabras de ALVAREZ-CIENFUEGOS, el artículo 18.4 CE legitima una lectura o interpretación de todo el Capítulo Segundo del Título I de la Constitución en «clave informática»[16].

Asimismo, el bien jurídico tutelado en la protección de datos no se identifica exclusivamente con la esfera íntima o privada de las personas, antes bien, al contrario, se extiende a garantizar otros valores y libertades de las personas, tal y como se indica en el art. 18.4 de la CE; y aún más, la protección de datos alcanza en el ordenamiento jurídico una dimensión institucional que se materializa en la configuración de autoridades específicas de control, al tiempo que se regulan procedimientos para la tutela de los nuevos derechos.

Por otra parte, se afirma con frecuencia que el derecho a la protección de datos constituye un medio o instrumento jurídico para la garantía de ejercicio de otros valores y principios de la persona, tales como la dignidad humana y el libre desarrollo de su personalidad, lo que se traduce en el desconocimiento de su identidad como derecho de la persona; ahora bien, precisamente por ser esto así, el derecho a la protección de datos alcanza la categoría de derecho fundamental, no en vano, todos los derechos fundamentales tienen vocación instrumental respecto de la dignidad y la personalidad humana.

---

[15] «[…] lo realmente grave aparece cuando esta información que puede dañar al honor incide en el ejercicio de los derechos por parte de los ciudadanos, es decir, cuando un ciudadano, por ejemplo, deseando constituir una asociación o promocionar una reunión, o bien practicar una actividad económica, encuentra que, por razón de una información de la que él no es conocedor y respecto de la cual no puede ni incluso pronunciarse en muchas ocasiones, se limita de tal manera el ejercicio de sus derechos que se ve colocado en una situación de inferioridad y desigualdad frente a los demás ciudadanos». Cfr. Enmienda núm. 117, Diario de sesiones del Congreso de los Diputados. Comisión de Asuntos Constitucionales y Libertades Públicas, núm. 70, 19 de mayo de 1978, p. 2527.

[16] ALVAREZ-CIENFUEGOS SUÁREZ, José M.ª, «El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos», *Actualidad Aranzadi,* núm. 37, 1991, pp. 457-465.

Ha de subrayarse igualmente que la consideración del derecho a la protección de datos como derecho fundamental facilita el reforzamiento de la tutela de los bienes y derechos que ampara, ya que permite articular una unidad de respuesta más adecuada ante el poder tecnológico, y ofrece a la persona mecanismos jurídicos concretos y específicos para la tutela de sus derechos frente al fenómeno informático. No olvidemos en este sentido, que los tradicionales derechos fundamentales tienen en su origen una configuración preinformática, que los pudiera hacer ineficaces para la defensa de los ciudadanos en la sociedad de la información. En efecto, desde una concepción tradicional de los derechos individuales, no es posible articular satisfactoriamente el sistema de protección de datos personales, ya que quedaría reducido a un derecho compensatorio y de naturaleza represiva. Y así, la consideración de derecho fundamental autónomo asegura un fortalecimiento de las garantías constitucionales, en tanto que permite la aplicación de cuantas medidas se reconocen constitucionalmente para la defensa de los derechos fundamentales, entre otras: el recurso de amparo, la intervención del Defensor del Pueblo, la vinculación inmediata a los poderes públicos para su tutela o el respeto al contenido esencial.

2.3. Perspectiva jurisprudencial de la protección de datos personales

Han sido numerosas y significativas las ocasiones en que el TC se ha manifestado a propósito del reconocimiento del derecho a la protección de datos, y si bien es cierto que en sus primeros pronunciamientos se mostró vacilante, sobre todo en lo referente a la denominación que identificaba a esta garantía constitucional, en los últimos tiempos, y principalmente después de la STC 202/2000, se muestra seguro en sus afirmaciones ya que primero, institucionaliza definitivamente el término derecho a la protección de datos, antes se había referido a la libertad informática; y segundo, define y delimita el concepto, la naturaleza jurídica y el contenido del derecho a la protección de datos[17].

La primera oportunidad en la que el TC se pronuncia sobre la naturaleza del derecho a la protección de datos en la STC 254/93 advierte claramente que «nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma que en último término no muy diferente a cómo fueron originándose e incorporándose históricamente los distintos derechos

[17] Cfr. STC 254/93, de 20 de julio y STC 202/99, de 8 de noviembre.

fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es en sí 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…». Confirman esta línea jurisprudencial posteriores resoluciones en las que explícitamente el TC se ha referido al derecho a la protección de datos como derecho fundamental (SSTC 11/98 y STC 292/2000).

Una cuestión que había resultado polémica era la vinculación que unía al derecho a la intimidad y a este nuevo derecho a la protección de datos, pues no debe olvidarse que no pocos juristas defienden que este último derecho no es sino una manifestación del derecho a la intimidad. En este punto, el TC se había mostrado cauteloso y pudiera decirse que había declinado manifestarse explícitamente; sin embargo, se rompe esta tendencia jurisprudencial cuando en la STC 292/2000 se detiene a delimitar y definir los difusos límites que separan el derecho a la intimidad y el derecho a la protección de datos, y establece que «este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consisten en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art.18.1CE), bien regulando su ejercicio (art. 53.1). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

En definitiva, a juicio del Tribunal Constitucional puede decirse que si el derecho a la intimidad aspira a garantizar al individuo un ámbito de reserva, y excluirlo del conocimiento ajeno, el derecho a la protección de datos reconoce a la persona un poder de control sobre la información personal que le concierne, sobre su utilización y destino, para evitar utilizaciones ilícitas. Así, tal y como ha declarado el TC, «el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal, es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos». Asimismo, y siguiendo las afirmaciones del TC, el objeto de protección del derecho fundamental a

la protección de datos no se limita a datos íntimos, sino a cualquier información personal, sea o no íntima, siempre que su tratamiento pueda afectar a derechos y libertades de la persona, sean o no fundamentales, «ya que su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos».

Finalmente, otra cuestión a la que ha prestado especial atención la jurisprudencia constitucional es la relativa al contenido esencial del derecho a la protección de datos, entendiendo por tal «aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles que dan vida al derecho resulten real, concreta y efectivamente protegidos» (STC 11/1981, 8 de abril). Una primera aproximación al contenido de este derecho permite afirmar que del enunciado literal del art. 18.4 CE se configura un contenido negativo, de limitación del uso de la informática, con lo que se erige en límite constitucional para el ejercicio de otros derechos; ello no obstante, no agota aquí su contenido este derecho, por cuanto que como ha declarado el TC «adopta además un contenido positivo, en forma de derecho de control sobre los datos relativos a la propia persona» (STC 254/93). En efecto, para el TC «resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y en su caso, requerirle para que rectifique o los cancele» (STC 292/2000).

En resumen, si bien es cierto que el derecho a la protección de datos nace vinculado a la idea de intimidad, ha de superarse esta concepción y avanzar en el reconocimiento de un nuevo derecho fundamental, que en la actualidad se configura a partir de la atribución de un haz de facultades de actuación y control que permiten a la persona decidir sobre la información que le concierne. Por tanto, la protección de datos no constituye una manifestación más del derecho a la intimidad, sino que como instrumento jurídico de tutela de la dignidad y el libre desarrollo de la personalidad alcanza en el ordenamiento jurídico sustantividad propia, y se configura como derecho a la personalidad.

II. **La protección de datos personales en el marco de la Unión Europea**

Si para el estudio del derecho a la protección de datos en el ordenamiento jurídico español es forzoso el análisis de la nueva Ley Orgánica 15/99 de Protección de Datos Personales, resulta igualmente inexcusable el estudio de la Directiva 95/46/CE de protección de datos, no en vano constituye el antecedente de la actual legislación, y delimita sin duda un marco regulador de protección de datos personales ineludible para el legislador español.

1. *La Directiva 95/46/CE de la protección de las personas frente al tratamiento de sus datos personales y de la libre circulación de esos datos*

1.1. Disposiciones generales. Especial referencia al objeto y ámbito de aplicación

Tal y como reza en el art. 1.1 de la Directiva 95/46/CE los Estados miembros garantizarán «la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales». A propósito de esta proclamación hay que subrayar en primer lugar que la Directiva no reduce su objeto a la tutela de la intimidad, sino que se refiere a la protección de las libertades y derechos fundamentales de las personas físicas, luego su protección no ampara a las personas jurídicas; y en segundo lugar, la protección de las personas tiene lugar no sólo frente a tratamientos automatizados, sino frente a cualquier tratamiento, automatizado o no.

Por otra parte, desde el ámbito comunitario siempre se ha mostrado especial sensibilidad por conciliar la protección de datos con la libre circulación de datos personales, y así, esta preocupación se ha manifestado en la Directiva 95/46/CE que en su art. 1.2 previene que «los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en el apartado 1». Por ello, la Directiva no se presenta como un texto restrictivo para la circulación de datos personales en el ámbito comunitario, antes bien, al contrario, como el propio título de la Directiva revela, el verdadero espíritu que animó la elaboración del texto comunitario no fue otro que servir de instrumento para el libre flujo de datos personales en la Unión Europea.

Respecto al ámbito de aplicación, señala el art. 3 que «las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». Por tanto, dos conceptos definen el ámbito de aplicación de la Directiva: por un lado, el concepto de tratamiento de datos, ya que la Directiva será aplicable a todo tratamiento automatizado o no; y por otro, el concepto de fichero, porque si el tratamiento no es automatizado la Directiva se aplicará cuando los datos estén contenidos en un fichero o sean destinados a ser incluidos en un fichero. La inclusión de los ficheros convencionales en el ámbito comunitario responde a la exigencia de que «la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión; que no obstante en lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas» (Considerando 27 de la Directiva 95/46/CE).

Ahora bien, las normas comunitarias no se aplicarán al tratamiento de datos personales:

a) efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los Títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;
b) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Por otra parte, para resolver la problemática sobre la legislación aplicable, la Directiva subraya que «el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva» (Considerando 20 Directiva 95/46/CE). Por tanto, los Estados miembros aplicarán las normas nacionales aprobadas para la adaptación de la Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento se efectúe en el marco de las actividades de un establecimiento del responsable en el territorio del Estado miembro. Cuando esté establecido en varios territorios deberá garantizar que cada establecimiento cumple las obligaciones previstas por el Derecho nacional aplicable;
b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en el lugar en que se aplica su legislación nacional en virtud del derecho internacional público;
c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento a medios situados en el territorio de dicho Estado miembro, salvo que los medios se utilicen sólo con fines de tránsito por el territorio comunitario. Deberá en este caso designarse un representante establecido en el territorio del Estado miembro, sin perjuicio de las acciones que correspondan contra el responsable del tratamiento.

A efectos de lo dispuesto en la Directiva se ha de entender por establecimiento «el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es factor determinante al respecto» (Considerando 19 Directiva 95/46/CE).

1.2. Condiciones generales para la licitud del tratamiento de datos personales

En principio, la Directiva reconoce en su art. 5 a los Estados miembros la facultad de prever, con independencia de las normas generales, condiciones especiales de licitud para tratamientos de datos personales en sectores específicos y en relación con categorías especiales de datos. En consecuencia, los Estados pueden establecer un reforzamiento en los mecanismos de protección de los derechos de las personas frente al tratamiento de datos, si bien este fortalecimiento nunca podrá implicar un obstáculo al libre flujo de información en el marco comunitario, ya que tal y como explícitamente previene la Directiva en la Exposición de Motivos «el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros».

1.2.1. El principio de calidad de los datos personales

Según proclama el art. 6 de la Directiva 95/46/CE los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre que los Estados miembros establezcan garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; se tomarán todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o tratados posteriormente, sean suprimidos o rectificados;
e) conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten posteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un periodo más largo del mencionado, con fines históricos, estadísticos o científicos.

Entre los principios que deben considerarse en el tratamiento de datos personales la Directiva 95/46/CE configura el principio de finalidad, según el cual los fines en el momento de recabar los datos deberán ser determinados, explícitos y legítimos, bien entendido que posteriormente no será posible su utilización para fines incompatibles con los inicialmente determinados; no será incompatible el tratamiento posterior «con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas», entendiendo por tales aquellas que impidan que los datos sean utilizados para tomar medidas o decisiones contra cualquier persona (Considerando 29 Directiva 95/46/CE).

También se ocupa la Directiva de definir el principio de proporcionalidad del tratamiento, de suerte que establece la necesidad de que la información personal sea adecuada, pertinente y no excesiva con relación a los fines para los que se recabe y trate posteriormente. Por tanto, el tratamiento sólo será lícito cuando la información obtenida sea proporcionada y necesaria para los fines del tratamiento. Asimismo, los datos personales deberán ser exactos, esto es, correctos, y en todo caso, responderán a la realidad del sujeto en cada momento, por lo que cuando sea necesario deberán actualizarse. Ciertamente, no debe menospreciarse la trascendencia de este principio, un dato incorrecto, incompleto o que es obsoleto no permite cumplir con la fina-

lidad del tratamiento de que se trate, y puede perjudicar gravemente al titular de los datos, porque ofrece una información inexacta que no se corresponde con las circunstancias reales, por lo que deberá ser rectificada o en su caso suprimida.

1.2.2. Principios relativos a la legitimación del tratamiento de datos personales

Exige la Directiva 95/46/CE en su art. 7 que los Estados miembros sólo autoricen un tratamiento de datos personales cuando:

a) el interesado ha dado su consentimiento inequívoco, o
b) es necesario para la ejecución de un contrato en el que es parte el interesado, o para la aplicación de medidas precontractuales a petición del interesado, o
c) es necesario para cumplir una obligación jurídica del responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para cumplir una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o al tercero cesionario, o
f) es necesario para la satisfacción del interés legítimo del responsable del tratamiento o del tercero a quien se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección de acuerdo al art. 1.1 de la Directiva 95/46/CE.

No pocas dudas presentaba para la doctrina la cuestión relativa a las condiciones que todo tratamiento debía cumplir de acuerdo con las prescripciones del texto comunitario. En efecto, si un tratamiento sólo se autorizaba cuando se dieran las circunstancias del art. 6 salvo en el caso de datos sensibles o de tratamiento de datos con fines exclusivamente periodísticos o de expresión artística y literaria, ¿Cuándo será aplicable el art. 7? Por otra parte, si el tratamiento de datos reúne las condiciones del art. 6 ¿Deberá además cumplir las disposiciones del art. 7? Y respecto a los datos sensibles, ¿qué norma será de aplicación? ¿Deberán observarse las disposiciones del art. 8 y además también las establecidas en el art.7? Los datos personales, según las prescripciones de la Directiva, deberán adecuarse a los principios de calidad previstos en el art. 6; pero, además, un tratamiento no será autorizado si no se cumplen las condiciones de los arts. 7 y 8. Así, ambas normas han de observarse; por una parte, los principios que hacen referencia a la información, y por otra parte, las condiciones

de licitud del tratamiento mismo. Y excepcionalmente, cuando la información objeto de tratamiento sea sensible deberán cumplirse las exigencias del art. 8.

Particularmente, en el caso de tratamientos con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán exenciones o excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que regulan la libertad de expresión (art. 9 Directiva 95/46/CE). Ya advirtió HEREDERO HIGUERAS de la dificultad para conciliar los usos y prácticas de los medios de comunicación con las exigencias de un sistema de protección de datos, lo que llevado a su extremo pudiera significar a juicio del autor la desaparición misma de las Agencias de prensa, y la imposibilidad de recabar, registrar y procesar noticias[18].

1.2.3. Categorías especiales de tratamientos

Los datos personales son objeto de protección por su relación con la persona, porque conciernen a aspectos de naturaleza privada; pero, destaca una categoría especial de información personal, aquella que concierne a los aspectos y derechos más esenciales de la persona, lo que les hace merecedores de una especial protección. Así lo ha defendido la Directiva 95/46/CE al indicar que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no serán objeto de tratamiento alguno, salvo cuando el interesado haya dado su consentimiento explícito (Considerando 33). Por ello, exige su art. 8.1 que los Estados miembros prohiban el tratamiento de «datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos así como el tratamiento de datos relativos a la salud».

En consecuencia, el principio general sobre el tratamiento de los datos sensibles es la prohibición del mismo; bien es verdad que se contemplan importantes excepciones a este principio, cuando concurren las condiciones de licitud establecidas en los apartados 2 a 5 del art. 8 de la Directiva. Así, pues, la prohibición general de tratamiento de los datos sensibles no se aplicará cuando el tratamiento:

a) haya sido consentido explícitamente, salvo que la legislación nacional disponga que la prohibición establecida no pueda levantarse con el consentimiento del interesado, o

---

[18] HEREDERO HIGUERAS, Manuel, *Directiva comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Pamplona, 1997, pp. 131-132.

b) sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en el ámbito laboral, en la medida en que esté autorizado por la legislación, y ésta prevea garantías adecuadas, o
c) sea necesario para tutelar el interés vital del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para prestar el consentimiento, o
d) se realice en el curso de las actividades legítimas y con las garantías adecuadas por una fundación, asociación o cualquier otro organismo sin fin lucrativo, cuya finalidad sea política, filosófica, religiosa o sindical, referido exclusivamente a sus miembros o a personas que mantengan contactos regulares con dichas entidades, y siempre que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
e) se refiera a datos que el interesado ha hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Cabe objetar a las excepciones anteriormente señaladas la ambigüedad de sus términos, lo que provoca no pocas inseguridades jurídicas y conlleva importantes dificultades en torno a la delimitación de los supuestos excepcionales. Así, por ejemplo, qué se entiende por personas que mantienen contactos periódicos con entidades sin fin de lucro, o en su caso, qué significa que los datos se «hacen manifiestamente públicos».

Por otra parte, introduce el art. 8.4 una excepción de carácter general, de suerte que siempre que se dispongan las garantías adecuadas, podrán los Estados «por motivos de interés público importantes» establecer otras excepciones. Se trata de una cláusula abierta que introduce una excepción a través de un concepto jurídico indeterminado, que sólo la lectura del Considerando 35 de la Directiva ayuda a delimitar cuando indica que «el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas conocidas oficialmente, se realiza por motivos importantes de interés público. […] si en el marco de las actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas». Por su parte, la Propuesta modificada de Directiva de 1992 manifestó también de forma explícita qué

debía entenderse por motivos de interés público importantes, al identificarlo con la denominada «cláusula humanitaria», estableciendo que las excepciones por motivos de interés público debían concederse a organismos internacionales de derechos humanos[19].

En otro orden de consideraciones, el art. 8.3 respecto a los datos de la salud dispone que la prohibición de tratamiento de tales datos sensibles no se aplicará «cuando el tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto». Por tanto, dos son las condiciones impuestas para la aplicación de la excepción: por un lado, que la finalidad del tratamiento se corresponda con lo establecido expresamente en el art. 8.3; y por otro lado, que quien realice el tratamiento sea una persona determinada, legitimada legalmente. Y así, se prevé tal y como advierte el Considerando 34 de la Directiva 95/46/CE que «se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida de las personas».

Finalmente, la Directiva en el art. 8.5 establece el régimen jurídico del tratamiento de una categoría especial de datos personales, los referidos a infracciones, condenas penales o medidas de seguridad, de suerte que el tratamiento de tales datos sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro, basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Bien es verdad que el registro completo de condenas penales sólo podrá llevarse bajo control de la autoridad pública. Se trata de evitar que a la condena penal

[19] Cfr. COM (92) 422, p. 19.

se sume una condena social que dificulte la reinserción del afectado en la vida cotidiana. Cierto es que han sido numerosas las dudas que ha planteado la expresión «bajo control de la autoridad pública»; luego, pueden ser dos las posibles interpretaciones: por un lado, que los datos puedan estar registrados en ficheros privados, pero que necesariamente la Administración establecerá las medidas de control del tratamiento, si bien el fichero podrá ser gestionado por tercero; o por otro lado, que los datos han de ser tratados en ficheros de titularidad pública, gestionados y controlados por la Administración[20]. En su caso, los Estados miembros podrán exigir que los tratamientos de datos relativos a sanciones administrativas o procesos civiles se realicen bajo control público.

Por último, aborda la Directiva el debate en torno a la autorización de los denominados «códigos únicos de identificación», cuestión que fue precisamente la que impulsó la aprobación de las numerosas legislaciones europeas de protección de datos, por el temor a su implantación generalizada sin garantías para los ciudadanos. Y en este sentido, nada nuevo dispone la Directiva que se limita a recordar que los Estados miembros determinarán las condiciones en que pueda ser objeto de tratamiento un número nacional de identificación o cualquier otro medio de identificación. La realidad ha venido a demostrar la imposibilidad de prohibir el tratamiento de tales datos, no en vano de forma paulatina la Administración ha atribuido de manera uniforme el número de identificación; ahora bien, esta licencia comunitaria no debe interpretarse en el sentido de que tales datos no se sujetan a las prescripciones comunitarias, bien al contrario, su tratamiento, en tanto que se trata de datos personales deberá someterse a las condiciones y garantías previstas en la Directiva 95/46/CE.

1.2.4. La información al interesado y el derecho de acceso a sus datos

Para establecer el auténtico alcance y significado de estos derechos es preciso indicar que el derecho a la información en el sistema de protección de datos constituye el fundamento necesario para el ejercicio de los demás derechos reconocidos, en otro caso, será imposible que los interesados puedan ejercitar los derechos de acceso, de oposición o el derecho a la rectificación y bloqueo de los datos personales.

---

[20] Resultan especialmente interesantes en este sentido las afirmaciones de PRIETO GUTIÉRREZ, «La Directiva 95/46/CE como criterio unificador», *Revista del Poder Judicial,* núm. 48, 1997, p. 178.

En la Directiva el derecho de información se manifiesta desde una doble perspectiva: derecho a la información cuando los datos se obtienen del propio interesado, y derecho a la información cuando los datos no se han recabado del interesado. Así, los Estados miembros dispondrán que el responsable o su representante deberán comunicar al interesado de quien se recaben los datos, por lo menos la información que a continuación se enumera, salvo si la persona ya ha sido informada (art. 10):

a) la identidad del responsable del tratamiento, y en su caso, de su representante;
b) los fines del tratamiento de que serán objeto los datos
c) cualquier otra información que según las circunstancias concretas resulte necesaria para garantizar un tratamiento leal de datos, y así información como:

—los destinatarios o categorías de destinatarios de los datos
—la obligación o no de responder, y las consecuencias de la negativa a responder
—la existencia de derechos de acceso y rectificación de sus datos.

Como quiera que la norma anteriormente transcrita es norma de mínimos, los Estados deben imponer sus previsiones para el efectivo cumplimiento del derecho de información, pero nada impide que además establezcan en su derecho interno una obligación más amplia de información al interesado cuando las circunstancias específicas así lo requieran.

Claro que el derecho de información se encuentra también reconocido cuando los datos no se obtienen del interesado, y a tal efecto proclama el art. 11 de la Directiva que los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar en el momento de la primera cesión de datos, comunicar al interesado, a no ser que ya hubiera sido informado, la misma información —salvo la relativa al carácter obligatorio o no de la respuesta y las consecuencias de una negativa a responder— que cuando los datos se recaban del propio interesado y que se establece en el art. 10 de la Directiva.

En efecto, que los datos personales no se obtengan del interesado no exime al responsable del tratamiento de informar a aquél de las circunstancias necesarias para hacer efectivos cuantos derechos reconoce al interesado el texto comunitario. Que los datos se obtengan de un tercero que no es su titular no significa que dicha publicidad habilite legalmente

al responsable para su tratamiento; cierto que la obligación de informar al interesado cesa cuando el registro o la comunicación están expresamente previstos por ley o si resulta imposible informarle, o cuando implica esfuerzos desproporcionados, como puede suceder cuando el tratamiento se realiza con fines históricos, estadísticos o científicos y siempre que se establezcan las garantías apropiadas (art.11.2 Directiva 95/46/CE)

Ahora bien, lo cierto es que el acceso del interesado a sus datos y a la información relativa al tratamiento resulta también esencial para facilitar el ejercicio de cuantos derechos le reconoce el ordenamiento para la tutela de sus datos. Por ello, establece el art. 12 de la Directiva 95/46/CE que los Estados deberán garantizar que el interesado obtenga del responsable del tratamiento, sin restricciones, ni gastos excesivos:

a) la confirmación de la existencia o no del tratamiento de datos que le conciernen, y la información de los fines del tratamiento, de las categorías de datos y de los destinatarios a quienes se comuniquen los datos;
b) la comunicación de forma inteligible de los datos objeto de tratamiento, así como de la información referida al origen de los datos
c) el conocimiento de la lógica utilizada en los tratamientos automatizados de datos referidos al interesado, en los casos de decisiones automatizadas.

Toda vez que se ha accedido a los datos objeto de tratamiento y a las demás circunstancias relativas al tratamiento, puede suceder que los datos sean incompletos o erróneos, o que el tratamiento sea ilícito; si así aconteciera, podrá ejercitarse el derecho de rectificación o cancelación, y el derecho de bloqueo de los datos, cuando el tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos (art. 12 Directiva 95/46/CE). Asimismo, el responsable del tratamiento deberá notificar a los terceros a quienes se hayan comunicado los datos la rectificación, supresión o bloqueo efectuado, a no ser que resulte imposible o suponga un esfuerzo desproporcionado.

1.2.5. Excepciones y limitaciones al ejercicio de los derechos

Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos reconocidos al interesado cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado, la defensa y la seguridad pública;

b) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
c) un interés económico y financiero importante de un Estado miembro de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
d) una función de control, de inspección o reglamentaria relacionada con el ejercicio de la autoridad pública a que hacen referencia los anteriores apartados;
e) la protección del interesado o de los derechos y libertades de otras personas.

A propósito de estas excepciones, la Directiva 95/46/CE, como ya hiciera el Convenio 108 del Consejo de Europa, advierte en la Memoria Explicativa que «las excepciones establecidas en esta disposición han de venir determinadas por la necesidad de salvaguardar los valores fundamentales de una sociedad democrática y tienen que adoptarse por ley».

Por otra parte, los Estados miembros «podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante disposición legal los derechos contemplados en el art. 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un periodo que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas» (art. 13.2 Directiva 95/46/CE).

Por tanto, las excepciones sólo podrán establecerse mediante disposición legal, cuando no concurra riesgo para el derecho a la intimidad, y se adopten complementariamente garantías oportunas. Coincidimos con PRIETO GUTIÉRREZ cuando afirma que estas excepciones responden a la necesidad de tutelar un conjunto de intereses de carácter público o general, que deben prevalecer frente a intereses particulares, lo que no debe significar una merma en los derechos de las personas en el tratamiento de sus datos personales[21].

1.2.5. El derecho de oposición al tratamiento

Se contempla en la Directiva 95/46/CE un derecho de oposición restringido a determinados supuestos, y no un derecho de oposición general;

[21] PRIETO GUTIÉRREZ, José M.ª, «La Directiva 95/46/CE como criterio unificador», *art. cit.*, pp. 181-182.

así, el art. 14 de la Directiva 95/46/CE dispone que los Estados miembros reconocerán derecho a:

a) oponerse en los casos del art. 7 apartados e) y f), en cualquier momento y por razones legítimas propias de su situación particular, a que sus datos sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;
b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por vez primera a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos a dicha comunicación o utilización. A estos efectos, los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia de este derecho.

El primero de los supuestos, introduce la oposición por razón del tratamiento, y contempla la utilización de los datos con determinados fines, si bien la oposición aun por razones legítimas no será posible cuando el tratamiento esté autorizado legalmente. El segundo de los supuestos, puede inducir a confusión cuando plantea en términos que parecen alternativos el derecho de oposición y el de información; bien es verdad, que el derecho de información al interesado constituye una condición previa y necesaria para el posterior ejercicio del derecho de oposición. Por tanto, la información al interesado del tratamiento con fines de prospección no excluye en modo alguno el reconocimiento y ejercicio del derecho de oposición.

1.2.6. Decisiones individuales automatizadas

El reconocimiento de este derecho en el ámbito comunitario tiene su más inmediato antecedente legislativo en la Ley francesa de 1978, si bien se introducen importantes novedades respecto al texto francés. Así, dispone el art. 15 de la Directiva que los Estados miembros reconocerán a las personas el «derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etcétera». Este

principio general encuentra dos excepciones, por lo que las personas deberán someterse a decisiones individuales automatizadas cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguarda de su interés legítimo; o
b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

La norma provocó cierta intranquilidad a las empresas de marketing directo, ya que en consideración a estas disposiciones, se cuestionaba la licitud de las prácticas y usos de estas empresas, consistentes en seleccionar destinatarios a partir de determinada puntuación obtenida por ordenador, lo que facilita la tarea de formar listados o relaciones de destinatarios con fines de publicidad directa.

A propósito de las excepciones que se incorporan, significar su escasa relevancia práctica, ya que en ningún caso se traducen en garantías jurídicas importantes para el interesado. En efecto, el derecho del interesado a ser oído no establece otras consecuencias que no sean las de hacerse escuchar; y por otra parte, cuando el tratamiento esté autorizado, si bien se exigen garantías y medidas únicamente se indica que deberán ser «apropiadas», sin que en ningún caso se especifique en qué deberán consistir o cómo han de adoptarse tales medidas.

1.2.7. Confidencialidad y seguridad del tratamiento

Respecto a la confidencialidad del tratamiento el art. 16 de la Directiva 95/46/CE restringe el tratamiento de los datos a los que tengan acceso, a las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal. De lo expuesto se desprende que el deber de confidencialidad se configura no como una obligación de secreto profesional, sino como un deber legal de sujetarse en su actuación a las instrucciones y directrices del responsable del tratamiento; claro que en realidad la obligación de seguir las instrucciones del responsable no se limita a la obligación de confidencialidad, sino a cualesquiera otros aspectos relacionados con el tratamiento.

Por otra parte, los Estados miembros impondrán al responsable del tratamiento la obligación de «aplicar las medidas técnicas y de organi-

zación adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales». Estas medidas de protección garantizarán, atendiendo los conocimientos técnicos existentes y el coste de su aplicación, un nivel de seguridad adecuado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban tutelarse.

Así, también, la Directiva 95/46/CE define las medidas de seguridad técnicas tanto cuando el tratamiento se realiza por el propio responsable como cuando se ejecuta por encargo. En el primero de los supuestos, el responsable deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnicas y de organización de los tratamientos que deban efectuarse, y se asegure del cumplimiento de las medidas. Cuando el tratamiento se realiza por encargo, deberá estar regulado por un contrato u otro acto jurídico, que constará por escrito o forma equivalente a efectos de conservación de la prueba, y vinculará al encargado del tratamiento con el responsable, y que disponga que:

—el encargado actuará según instrucciones del responsable del tratamiento;
—las obligaciones del art. 17.1 incumben también al encargado del tratamiento.

1.3. Las medidas y controles previos al tratamiento. La publicidad del tratamiento

Para cumplir con el principio de transparencia del tratamiento es preciso que se establezcan unos procedimientos de notificación a la autoridad de control que aseguren la publicidad de los fines y características de los tratamientos, para que pueda ejercerse un control sobre los tratamientos de datos. Por ello, el art. 18 de la Directiva 95/46/CE impone a los responsables del tratamiento la obligación de notificación a la autoridad de control con anterioridad a la realización de los tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

La obligación de notificación responde a una doble finalidad: por una parte, constituye un medio para posibilitar el ejercicio de los derechos de información y acceso por los interesados; y por otra parte, facilita el cumplimiento de la obligación de vigilancia e intervención de las

Autoridades de control respecto de los tratamientos de datos personales. Claro que «para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que precisen sus límites» (Considerando 49 Directiva 95/46/CE). Y así, siguiendo tales afirmaciones, podrán disponerse notificaciones simplificadas e incluso omitirse la notificación cuando:

a) para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los afectados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines del tratamiento, los datos o categorías de datos tratados, categoría o categorías de interesados, destinatarios a quien se comuniquen los datos y el período de conservación de los datos, y/o
b) el responsable del tratamiento designe, de acuerdo con su Derecho nacional, un encargado de protección de datos que tenga por cometido:

   —hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,
   —llevar un registro de los tratamientos efectuados por el responsable del mismo que contenga la información citada en el art. 21.1, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos de los interesados.

c) el tratamiento tenga por única finalidad llevar un registro que en virtud de disposiciones legales o reglamentarias esté destinado a facilitar información y estén abiertos a la consulta por el público en general o por toda persona con interés legítimo
d) el tratamiento sea efectuado en el curso de actividades legítimas con las debidas garantías por una fundación, asociación o cualquier entidad sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical y se refiera exclusivamente a sus miembros o a personas que mantengan con ellas contactos regulares y siempre que los datos no se comuniquen a terceros sin el consentimiento de los interesados.
e) el tratamiento de datos personales sea no automatizado se podrá disponer su notificación de forma simplificada.

Respecto al procedimiento de notificación, cada Estado miembro determinará el proceso y la forma de notificación de los tratamientos, si bien la Directiva establece en su art. 19 un contenido mínimo que deberá hacerse constar en la notificación, a saber:

- —nombre y dirección del responsable del tratamiento o de su representante
- —el o los objetivos del tratamiento
- —descripción de la categoría o categorías de interesados y de los datos o categorías de datos objeto del tratamiento
- —destinatarios o categorías de destinatarios a los que puedan comunicarse datos
- —transferencias de datos previstas a países terceros
- —descripción general que permita evaluar de modo previo si las medidas de seguridad adoptadas en aplicación de la Directiva resultan adecuadas.

Asimismo, se establecen otras medidas de control de los tratamientos, en particular, y para categorías especiales de tratamientos, señala la Directiva en su art. 20 que «Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán porque sean examinados antes del comienzo del tratamiento». Corresponde a la autoridad de control, o en su caso, al encargado del tratamiento proceder a la comprobación sobre los riesgos del tratamiento; también los Estados podrán realizar dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las garantías oportunas. Cierto que la propia Directiva indica cuáles pueden ser considerados tratamientos especialmente peligrosos para los derechos y libertades, y cita entre otros los que pueden excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, o los relativos al uso particular de una tecnología nueva.

Cabe objetar a la norma comunitaria que no haya previsto las consecuencias que puedan derivarse de este control previo, si bien puede arrojar luz sobre esta cuestión el Considerando 54 de la Directiva cuando indica que «tras dicho control previo la autoridad de control, en virtud de lo que disponga su derecho nacional, podrá emitir un dictamen o autorizar el tratamiento de datos»; pero, ¿qué efectos se derivarán de este dictamen? ¿Tendrá carácter preceptivo? Y en su caso, ¿Qué medidas deberán adoptarse para darle cumplimiento?

Asimismo, acoge el art. 21 de la Directiva 95/46/CE el principio de publicidad del tratamiento, cuando establece la necesidad de que se

adopten para ello las medidas necesarias y exige a la autoridad de control que realice un registro de los tratamientos notificados y de las informaciones mínimas a las que el texto comunitario obliga. Registro que ha de ser público y de general consulta. Claro que no hay que olvidar que determinados tratamientos de datos personales quedan excluidos de la obligación de notificación; en estos casos, los responsables del tratamiento o el órgano designado por cada Estado miembro, comunicará en la forma adecuada a quien lo solicite la información mínima respecto al tratamiento (art. 19.1 Directiva 95/46/CE). Sin embargo, la norma encuentra una excepción en los tratamientos cuyo fin único sea llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

Sorprende que el texto comunitario no delimite explícitamente la persona obligada a cumplir con el principio de publicidad en los casos de tratamientos de notificación no obligatoria, por cuanto que el cumplimiento del principio de publicidad constituye un elemento esencial del contenido del derecho a la protección de datos, que queda sin embargo en cuanto a su eficacia a merced de las decisiones de cada Estado.

1.4. Recursos judiciales, responsabilidad y sanciones

Como ya hiciera el Convenio 108 del Consejo de Europa en su art. 10, la Directiva obliga a los Estados miembros a establecer los recursos y sanciones necesarias para los supuestos de infracción de las disposiciones de derecho interno que den cumplimiento a los principios fundamentales de protección de datos personales. Por ello, dispone el art. 22 de la Directiva 95/46/CE que sin perjuicio de los recursos administrativos que puedan corresponder, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que garanticen las disposiciones nacionales aplicables a cada tratamiento.

Respecto al régimen de responsabilidad, garantiza la Directiva que aquella persona que sufra un daño como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva, tendrá derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. El responsable sólo se liberará de dicha obligación si demuestra que no se le puede imputar el hecho que ha provocado el daño, luego si prueba la responsabilidad del interesado o un caso de fuerza mayor

(Considerando 55 Directiva 95/46/CE). Y así, contrariamente a lo dispuesto en el Convenio 108 del Consejo de Europa, que no se detiene a establecer un régimen de responsabilidad por el tratamiento de datos, se traslada a la Directiva la preocupación de las numerosas legislaciones europeas de protección de datos que habían incorporado normas sobre responsabilidad en el tratamiento de datos, como es el caso de Alemania o Bélgica. Bien es cierto que la Directiva no establece un régimen de responsabilidad objetivo por la realización del tratamiento, tal y como se pretendía imponer por algunos países.

En relación con las sanciones, la Directiva reconoce a los Estados miembros autoridad para adoptar las medidas necesarias para la eficaz aplicación de las disposiciones comunitarias, y determinar las sanciones aplicables en caso de incumplimiento, indicando a este respecto que «deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la Directiva».

1.5. Transferencia de datos a terceros países

El principio general adoptado por la Directiva para la regulación de las transferencias de datos entre Estados es el de la autorización de tales transmisiones; ello no obstante, se han establecido ciertas excepciones a este principio general.

Se exige para autorizar las transferencias de datos a terceros países cuando sean objeto de tratamiento o estén destinados a ser objeto de tratamiento con posterioridad, que el tercer país «garantice un nivel de protección adecuado». El carácter adecuado del nivel de protección se valorará atendiendo a todas las circunstancias que concurran en la concreta transferencia de que se trate; pero, en particular, se atenderá a «la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países» (art. 25.2 Directiva 95/46/CE). En definitiva, para definir el nivel adecuado de protección parece necesario establecer antes cuál es el nivel inadecuado de protección, a lo que deberá contestarse que será aquél en el que se producen perjuicios para los interesados que permiten hablar de vulneración de su derecho a la protección de datos personales.

Resulta significativo que en este ámbito las previsiones de la Directiva no sigan los criterios establecidos en el Convenio 108 del Consejo de Europa, por cuanto que este último para las transferencias de datos

entre Estados adoptaba el principio de nivel de protección equivalente entre el Estado de origen y el de destino de los datos; por el contrario, la Directiva se refiere a un nivel de protección adecuado en el Estado destinatario de los datos, lo que sin duda debilita el grado de exigencia requerida en el Convenio 108 del Consejo de Europa. Así, cuando la Comisión compruebe que el tercer país no garantiza un nivel de protección adecuado, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales a dicho país, si bien en ese momento la Comisión iniciará los contactos y negociaciones necesarias para remediar la situación. De este modo, podrá hacer constar que un país tercero garantiza un nivel de protección adecuado a la vista de su legislación nacional o de los compromisos internacionales suscritos, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Claro que se contemplan importantes excepciones a la prohibición de transferencia de datos a tercer país que no garantice un nivel de protección adecuado, cuando la transferencia:

a) se haya consentido de forma inequívoca por el interesado, o
b) sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para ejecutar medidas precontractuales solicitadas por el interesado, o
c) sea necesaria para celebrar o ejecutar un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
d) sea necesaria o legalmente exigida para salvaguardar un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o
e) sea necesaria para la salvaguarda del interés vital del interesado, o
f) tenga lugar desde un registro público, que en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

De las excepciones anteriormente transcritas a la prohibición de transferencia de datos personales a país tercero, sorprende la constante utilización de conceptos jurídicos indeterminados, que contribuyen a incrementar la inseguridad jurídica e indefensión para los afectados. En este sentido, el Considerando 58 establece una relación de supuestos en los que se aprecia la existencia de «necesidades públicas importantes»; se mencionan entre otras, las transferencias internacionales entre

administraciones fiscales o aduaneras o los servicios de la seguridad social, o la transferencia desde un registro previsto legalmente para la consulta pública o por personas con interés legítimo, si bien en este último supuesto se advierte que «la transferencia sólo debería poder efectuarse a petición de dichas personas o cuando éstas sean destinatarias».

Además de las restricciones ya señaladas, el art. 26.2 de la Directiva contempla otra excepción general por la cual los Estados miembros podrán autorizar transferencias a país tercero que no garantice un nivel de protección adecuado cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, y del ejercicio de los respectivos derechos. De estas autorizaciones particulares se dará cuenta a la Comisión y a los demás Estados miembros; y, si un Estado o la Comisión se oponen justificadamente, por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas se adoptarán las medidas previstas en el art. 31 de la Directiva.

Facilita esta norma comunitaria la práctica de resolver caso por caso, a través de contratos o convenios entre responsables de los tratamientos, la autorización de transferencia de datos a terceros países que no garanticen nivel de protección adecuado. Bien es verdad que hemos de manifestar nuestras dudas sobre la oportunidad de estos usos, ya que en la medida en que se acuerdan entre los responsables, sin audiencia ni participación del interesado, podrán provocar situaciones de indefensión. En efecto, la utilización de cláusulas contractuales excepcionales puede favorecer que se reduzcan las condiciones de licitud, máxime si piensa que al tratarse de contratos entre el responsable del tratamiento y el destinatario, el interesado sólo podrá invocarlos cuando se concierten como contratos a favor de tercero.

1.6. Los códigos de conducta

Es fácil comprender que el tratamiento de datos personales se manifiesta de forma diferente en determinados sectores, y presenta por ello caracteres que lo definen; así, parece deseable en tales sectores, que se procure establecer unas normas de uso profesional, códigos de conducta, para la tutela de los derechos de los interesados en el tratamiento de datos en tales sectores, lo que permitirá además una correcta aplicación de las disposiciones comunitarias y nacionales. Es por ello que la Directiva 95/46/CE en su art. 27 anima a los Estados miembros y a la Comisión a promover la elaboración de códigos de conducta desti-

nados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por cada Estado en aplicación de la Directiva. Cuando se hayan aprobado o elaborado códigos nacionales de conducta en determinados sectores podrán ser examinados por la autoridad de control, que velará porque dichas normas respeten y se sometan a las disposiciones nacionales de protección de datos. Sin embargo, critica la doctrina que se limite la Directiva a los códigos de conducta sectoriales, de forma que parece excluir la aprobación de códigos de conducta de empresas[22].

Por otra parte, respecto a los proyectos de códigos comunitarios, así como a sus modificaciones o prórrogas, podrán ser sometidos a examen del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, que habrá de pronunciarse sobre la conformidad de tales proyectos con las disposiciones nacionales adoptadas en aplicación de la Directiva. En cualquier caso, la Comisión podrá realizar publicidad de los códigos que hayan recibido un dictamen favorable del Grupo. Sorprende que la Directiva no establezca con carácter imperativo la obligación de publicidad para los códigos comunitarios, por lo que su publicación dependerá de la libre decisión de cada Estado.

1.7. La autoridad de control y el Grupo de protección de personas en lo que respecta al tratamiento de datos personales

La propuesta de Directiva de 1990 configuró a la autoridad de control como eje central de su sistema de protección de datos, bien es verdad que antes las legislaciones nacionales europeas hasta la fecha aprobadas ya habían introducido esta institución, si bien con importantes diferencias entre sí. En este contexto, la Directiva 95/46/CE atribuye a la autoridad de control la función de «vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva» (art. 28.1 Directiva 95/46/CE). En concreto, de las funciones que la Directiva atribuye a la autoridad de control destacan:

a) poderes de investigación, como el acceso a los datos objeto de un tratamiento o recabar información necesaria para el cumplimiento de su misión de control
b) poderes efectivos de intervención, como el de formular dictámenes antes de realizar los tratamientos, y garantizar una publicidad adecuada a dichos dictámenes, o el de ordenar el bloqueo

[22] Rubí Navarrete, Jesús, «Los códigos tipo: la alternativa de la autorregulación», *Actualidad Informática Aranzadi,* núm. 35, 2000.

o destrucción de datos, o prohibir un tratamiento, o dirigir una advertencia o amonestación al responsable del tratamiento, o someter la cuestión a los parlamentos o a otras instancias políticas

c) capacidad procesal frente a infracciones a disposiciones nacionales adoptadas en aplicación de la Directiva y para informar a la autoridad judicial de infracciones
d) conocer de las solicitudes de cualquier persona o asociación que le represente, en relación con la protección de sus derechos y libertades en el tratamiento de datos personales y entender de las solicitudes de control de la licitud del tratamiento que se presenten cuando sean de aplicación las disposiciones nacionales sobre excepciones y restricciones al ejercicio de los derechos de protección de datos
e) presentar periódicamente un informe sobre sus actividades
f) ser consultado en el momento de la elaboración de medidas reglamentarias o administrativas relativas a la protección de datos personales.

Asimismo, advierte el texto comunitario que estas autoridades deberán ejercer sus funciones con total independencia. Esto es, no se precisa que la autoridad de control sea una autoridad nacional de nueva creación, ni siquiera ha de ser independiente, sino funcionalmente independiente. Esta falta de compromiso del texto comunitario y la ambigüedad de sus afirmaciones en una cuestión tan trascendental para la protección de datos ha levantado no pocas críticas de la doctrina que ha tachado a la Directiva de falta de rigor y compromiso con la tutela de las personas[23].

Por su parte, las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, especialmente mediante el intercambio de información; no en vano la Directiva advierte que se podrá instar a la autoridad de control nacional a ejercer sus poderes desde otra autoridad nacional de otro Estado miembro. En este sentido, y si bien se debatió sobre la posibilidad de que las autoridades de control ejercieran sus funciones extraterritorialmente, a petición de un ciudadano nacional, esta idea fue descartada definitivamente, ahora bien, sí se reforzó la necesidad de cooperación entre autoridades.

---

[23] Hubiera sido oportuno que el texto comunitario sentara las bases para la regulación de una materia que tantas diferencias presentaba entre las legislaciones nacionales, de suerte que se armonizaran los principios para la configuración jurídica de las autoridades nacionales de control. Así lo ha entendido PRIETO GUTIÉRREZ, «La Directiva 95/46/CE como criterio unificador», *art. cit.,* p. 193.

La autoridad de control está llamada a desempeñar un papel esencial en la tutela de las personas, de ahí la exigencia de que sus miembros y agentes se sujeten, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso; obsérvese que esta obligación no se configura como una obligación legal, sino como un deber de secreto profesional.

Pero además de la autoridad de control, la Directiva configura otra institución, el denominado Grupo de protección de las personas en lo que respecta al tratamiento de datos personales (en adelante Grupo de protección), por lo que establece que dicho Grupo tendrá carácter consultivo e independiente. Estará integrado por un representante de la autoridad de control designada por cada Estado miembro, por un representante de la autoridad de control creada por las instituciones y organismos comunitarios y por un representante de la Comisión, siendo designados en su caso cada uno de ellos por la autoridad a la que representan.

Las funciones que el Grupo de protección tiene asignadas son de carácter consultivo y de asesoramiento, y entre otras destacan:

a) estudiar la aplicación de las disposiciones nacionales en la adaptación de la Directiva y formular a iniciativa propia recomendaciones sobre cualquier asunto relacionado con la protección de datos personales;
b) emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en los países terceros, y sobre códigos de conducta comunitarios;
c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales
d) informar a la Comisión sobre divergencias en los Estados miembros entre las legislaciones y la práctica que afecten a la equivalencia de la protección de las personas en lo referido al tratamiento de datos;
e) elaborar un informe anual sobre la situación de la protección de datos personales en la Comunidad, y en los países terceros.

Por tanto, el Grupo de protección se configura como una institución independiente, lo que se manifiesta en dos aspectos: por un lado, a través de la libre designación de sus representantes, que corresponde no a los Gobiernos nacionales, sino a las autoridades de control; y por otro lado, por el sistema de adopción de acuerdos, por mayoría simple. Por ello, el Grupo de protección no es únicamente un órgano de coo-

peración o coordinación de las autoridades de control, sino que sus funciones tienen entidad propia, y no se encuentran sujetas a la decisión de las autoridades de control nacionales.

2. *Directiva 2002/58/CE, de 12 de julio de 2002, sobre la privacidad y las comunicaciones electrónicas*

Han sido importantes y numerosos los esfuerzos de las instituciones comunitarias por adecuar a los avances tecnológicos normas que facilitaran la protección de las personas en relación con el tratamiento de sus datos personales. De ahí que la primera Directiva 97/66/CE sobre protección de datos en el sector de las telecomunicaciones[24] haya sido recientemente derogada por un nuevo texto que se «adapta al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas sea el mismo, con independencia de las tecnologías utilizadas»[25].

Por tanto, el imparable desarrollo de la sociedad de la información ha contribuido a la introducción de nuevos servicios de comunicaciones electrónicas, de suerte que resulta relativamente accesible para el usuario la utilización de redes móviles digitales y de internet, lo que en la práctica conlleva nuevas posibilidades en materia de tratamiento de datos personales, de ahí que, tal y como reconoce la Directiva 2002/58/CE, el éxito de su utilización y de su desarrollo transfronterizo se vincule en gran medida a facilitar el acceso de forma universal y a garantizar la intimidad del usuario y la confidencialidad de las comunicaciones.

2.1. Ambito de aplicación y objeto

Se aspira con esta Directiva a armonizar las disposiciones nacionales para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales, y en especial, del derecho a la intimidad,

---

[24] Cfr. Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DOCE núm. L 24, de 30 de enero de 1998.

[25] Cfr. Considerando 4 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, DOCE núm. L 201, de 31 de julio de 2002.

en lo que respecta al tratamiento de datos personales en el sector de las telecomunicaciones (art. 1 Directiva 2002/58/CE).

Ahora bien, la Directiva 2002/58/CE no será de aplicación a actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, ni a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. Asimismo, la Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad. Así, las normas relativas a identificación de la línea de origen y de la línea conectada y al desvío de llamada se aplicarán a las líneas de abonado conectadas a centrales digitales, y a las líneas de abonado conectadas a centrales analógicas siempre que sea posible técnicamente y no precise un esfuerzo económico desproporcionado; en todo caso, los Estados informarán a la Comisión de los supuestos en que no es posible técnicamente o exija esfuerzo económico desproporcionado cumplir con las condiciones legales (art. 3.3. Directiva 2002/58/CE).

2.2. Confidencialidad de las comunicaciones

En lo relativo a la seguridad de los servicios de comunicaciones electrónicas, las mayores dificultades se presentan en internet y en las comunicaciones a través de una red de telefonía móvil analógica, y por ello, los usuarios de estos servicios deberán estar convenientemente informados de los riesgos para la seguridad que escapan a posibles soluciones adoptadas por el proveedor del servicio; y en especial, se informará a los usuarios de internet de las medidas que puedan adoptar para proteger sus comunicaciones, si bien esta obligación no exime al proveedor de adoptar las medidas necesarias para restablecer el nivel de seguridad propio de estas comunicaciones.

La Directiva 2002/58/CE exige en su art. 5.1. que los Estados garanticen «la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de redes públicas de comunicaciones y de servicios de comunicaciones electrónicas disponibles al público». Se prohibe la escucha, grabación, almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los interesados, salvo cuando estén autorizados legalmente a tenor de lo dispuesto en el art. 15.1 de la Directiva 2002/58/CE.

Ello no obstante, se permite el uso de redes de comunicaciones electrónicas con fines de almacenamiento de información o de obten-

ción de acceso a la información almacenada en el equipo terminal de un usuario o abonado, cuando se les facilite información clara y completa, especialmente, sobre los fines del tratamiento de datos, y sobre el derecho de oposición al mismo reconocido al interesado en la Directiva 95/46/CE. Bien es verdad, que no se podrá impedir el almacenamiento o el acceso de naturaleza técnica con el solo fin de realizar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónica, o en la medida de lo estrictamente necesario para proporcionar a una empresa de información un servicio solicitado por el usuario o abonado. Abundando en lo expresado, advierte la Directiva que los equipos terminales de los usuarios de redes de comunicaciones electrónicas y la información en ellos almacenada pertenece a la esfera privada del usuario y por tanto, debe protegerse de acuerdo con las previsiones del Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales. Respecto a los programas espía o identificadores ocultos y otros dispositivos similares que pueden introducirse en el terminal del usuario, sin su conocimiento, para acceder a la información oculta o rastrear las actividades del usuario, únicamente será posible su utilización con conocimiento del propio usuario y para fines legítimos (Considerando 24 Directiva 2002/58/CE). La utilización de los denominados «cookies» o chivatos deberá supeditarse a la información al usuario sobre su uso, de forma que éste pueda impedir que se almacene en su equipo terminal dicho dispositivo, y en cualquier caso, su utilización responderá siempre a un fin legítimo.

Es por ello que como ha significado PRIETO ANDRES la nueva Directiva 2002/58/CE refuerza la protección de los ciudadanos en relación con su derecho a la intimidad en el ámbito de las comunicaciones electrónicas[26].

2.3. Protección de los usuarios en el tratamiento de datos personales

Respecto al tratamiento de datos del tráfico, entendiendo por tales aquellos tratados a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación, exige la Directiva el cumplimiento del principio de calidad de los datos, porque su tratamiento sólo será posible en relación con los datos necesarios a efectos de facturación y pago de interconexiones.

---

[26] Prieto Andrés, Antonio, «La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones», *La Ley,* núm. 5620, 2002.

De igual forma, se respetará el principio de finalidad en el tratamiento de estos datos, por cuanto que el mismo se autoriza sólo hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Excepcionalmente, cuando el proveedor informe de forma clara de los tipos de datos de tráfico tratados y de la duración del mismo, y previo consentimiento del abonado o usuario, que podrá ser revocado en cualquier momento, el proveedor podrá utilizar los datos del tráfico para la promoción comercial de servicios de comunicaciones o para la prestación de servicios con valor añadido, en la medida y durante el tiempo necesario para tales prestaciones o para la promoción comercial. Bien es verdad que la Directiva restringe el acceso y tratamiento de estos datos, de suerte que únicamente legitima a aquellas personas que actúen bajo autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de clientes, de la detección de fraudes, de la promoción comercial o de la prestación de un servicio de valor añadido, si bien en todo caso el tratamiento se ajustará a lo estrictamente necesario para la prestación de los servicios.

Por otra parte, los proveedores de servicios de comunicaciones electrónicas informarán a sus abonados de la existencia de la identificación de las líneas llamantes y conectadas, y de todos los servicios ofrecidos como consecuencia de la identificación de dichas líneas, así como sobre las diferentes opciones disponibles para garantizar la confidencialidad de los usuarios y abonados. Estas opciones no necesariamente han de ofrecerse como servicios usuales de la red automática, pero deberán obtenerse por la simple solicitud al proveedor.

Sobre las guías de abonados a los servicios de comunicaciones electrónicas, si bien se reconoce que constituyen un medio fundamental de publicidad para los usuarios, resultará necesario conciliar su utilización con el respeto a la intimidad de las personas físicas y el interés legítimo de las personas jurídicas, que exige que los abonados presten el consentimiento para la publicidad de sus datos personales en las guías[27]. Previamente, serán informados gratuitamente sobre los fines de las guías, y sobre cualquier uso particular que pueda hacerse de las versiones electrónicas, en especial a través de funciones de búsqueda incorporadas al soporte lógico.

---

[27] Sobre esta cuestión Cfr. Herrán Ortiz, Ana I., «La nueva Directiva europea 2002/58/CE sobre privacidad y comunicaciones electrónicas», *XVII Encuentros sobre Informática y Derecho,* Universidad Pontificia Comillas, Madrid, 2003.

Asimismo, el tratamiento de estos datos se adecuará al principio de proporcionalidad, por cuanto que los datos incorporados deberán ser pertinentes para la finalidad de la guía, teniendo derecho el abonado de forma gratuita a comprobar qué datos han sido incorporados, y en su caso, a que sean corregidos o suprimidos. En cualquier caso, el abonado gratuitamente tiene derecho a no ser incluido en la guía.

Por otra parte, la inclusión en las guías de datos distintos a los necesarios para la identificación de un usuario precisará el consentimiento específico. Así, también se informará al abonado de la finalidad de tales guías y de los posibles cesionarios cuando los datos puedan ser objeto de cesión; bien entendido que si quien recoge los datos los desea utilizar después con fines suplementarios deberá obtener nuevamente el consentimiento del abonado. Ahora bien, la Directiva no será de aplicación a ediciones de guías ya producidas o puestas en el mercado en forma impresa o electrónica no conectada antes de entrar en vigor las disposiciones adoptadas en virtud del nuevo texto comunitario (art. 16 Directiva 2002/58/CE).

2.4. Comunicaciones no solicitadas

Un problema importante para los usuarios ha sido el envío de comunicaciones no deseadas; en efecto, los abonados tienen derecho a que se garantice su intimidad frente a intromisiones no deseadas a través de comunicaciones no solicitas con fines de venta directa, especialmente mediante llamadores automáticos, faxes y mensajes de correo electrónico, incluidos los de SMS. Por ello, la Directiva 2002/58/CE exige para estas comunicaciones el consentimiento previo del abonado, que no expreso ni por escrito. Sin embargo, y pese al tenor literal del texto comunitario, significar que el consentimiento, siguiendo lo dispuesto en la Ley Orgánica 15/99, deberá ser inequívoco y consistir en una declaración de voluntad libre, específica e informada. Abundando en lo expresado, el art. 21 de la Ley de comercio electrónico apunta que el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente sólo podrán realizarse cuando previamente hayan sido solicitadas o expresamente consentidas por los destinatarios[28].

Excepcionalmente, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de una

[28] Cfr. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, BOE núm. 166, de 12 de julio de 2002.

venta o prestación de servicio, podrá utilizar dichas señas electrónicas para la venta directa de sus productos o servicios de similares características y siempre que se ofrezca con claridad a los clientes y sin cargo alguno, la posibilidad de oponerse a dicha utilización en el momento en que se recojan las mismas, y caso de que no se rechace inicialmente, cada vez que reciban posteriormente un mensaje. Queda prohibida la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule u oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que no tengan dirección válida para poder ejercer el derecho de oponerse al envío de los mensajes.

Propone también la Directiva otras medidas que consisten en sistemas mediante los cuales el usuario puede acceder a la identidad del remitente y al asunto objeto del mensaje, e incluso pueda borrar sin tener que descargar el contenido del mismo ni los ficheros anexos, con lo que se reducen costes para el usuario.

III. **La Ley Orgánica 15/99, de 13 de diciembre, de protección de datos personales**

Antes de presentar la actual Ley de protección de datos es preciso conocer las circunstancias que rodearon su aprobación, y por supuesto, comprender el fenómeno de la protección de datos personales que encuentra en España respuesta legal en los años 90 con la aprobación de la Ley Orgánica 5/92, de 29 de octubre (en adelante LORTAD)[29].

Puede decirse que ha sido largo el peregrinar de la nueva Ley Orgánica 15/99 de Protección de Datos (en adelante LOPD) por las Cámaras legislativas españolas, tanto como tortuoso ha sido el camino hasta su aprobación definitiva en 1999[30]. En efecto, en un principio se presentó como proyecto de modificación de la existente LORTAD, una técnica legislativa que vino a complicar la aprobación de la nueva legislación, y que no convenció a los Grupos Parlamentarios, que presentaron numerosas enmiendas, lo que reforzó la idea de que el nuevo texto debía adoptar la forma de Ley, y derogar la anterior legislación. Finalmente, por la oposición de los Grupos y por las importantes enmiendas al texto, tanto el Informe de la Ponencia, como el dictamen de la Comisión constitucional adoptan la forma de Ley orgánica.

En este sentido, no hay que olvidar que la propia Exposición de Motivos del proyecto de Ley, nos acerca a las consideraciones del legislador, sobre las que se sienta la aprobación de esta nueva ley, a saber: la LORTAD se ajustaba en su mayor parte a las disposiciones de la Directiva 95/46/CE, por lo que sólo se hace necesario un mínimo ajuste por el legislador español para acomodar la Directiva a nuestro ordenamiento. Sin embargo, no puede sostenerse esta idea sin que al mismo tiempo quiebren los principios más esenciales del sistema de protección de datos personales, era por tanto necesario, un nuevo texto que configurase desde una perspectiva más garantista y actual la protección de los derechos y libertades de la persona frente al tratamiento de sus datos personales[31].

Otra circunstancia que también condicionó la aprobación de la nueva Ley fue la presencia de los recursos de inconstitucionalidad, no resueltos entonces, a la entonces LORTAD, que alcanzaron respuesta a finales

---

[29] Cfr. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, BOE núm. 262, de 31 de octubre de 1992.

[30] Cfr. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE núm. 298, de 14 de diciembre de 1999.

[31] Herrán Ortiz, Ana I., *La violación de la intimidad en la protección de datos personales,* Dykinson, Madrid, 1999.

del año 2000, lo que significó que durante los debates que precedieron a la nueva Ley estuvieran muy presentes[32].

Así, pueden ser importantes los recelos y las críticas que suscita el nuevo texto, principalmente por la ambigüedad de algunas de sus disposiciones, o por la resistencia del legislador a incorporar nuevos fenómenos informáticos y técnicos al ámbito de protección de la Ley, no olvidemos que el texto constitucional impone al legislador una clara obligación: limitar el uso de la informática para garantizar los derechos y libertades de las personas. En las próximas páginas se intentará desvelar si la nueva legislación ha sido capaz de cumplir con el mandato constitucional o, por el contrario, si todavía son muchas las quiebras que presenta el sistema de protección de datos personales en el ordenamiento jurídico español.

1. *Los principios y garantías individuales de protección de datos*

Antes de examinar las garantías establecidas en la LOPD es importante definir los datos y los tratamientos a que afecta la Ley, en este sentido según dispone la LOPD ésta se aplica a los «datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado» (art. 2.1 LOPD).

Sin embargo, quedan excluidos del ámbito de aplicación de la Ley: a) los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; b) los ficheros sometidos a la normativa sobre protección de materias clasificadas; y c) los ficheros establecidos para la investigación de terrorismo y de formas graves de delincuencia organizada (art. 2.2 LOPD).

Los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos, y configuran un sistema de tutela que garantiza una utilización racional y razonable de los datos personales. Por ello a través de la configuración de estos principios el legislador aspira a constituir un sistema preventivo de tutela de la persona frente al tratamiento de sus datos, estableciendo un saludable equilibrio entre los avances de la sociedad de la información y el respeto a la libertad de los ciudadanos[33].

---

[32] Cfr. Diario de Sesiones del Congreso de los Diputados, Pleno y Diputación Permanente, VI Legislatura, núm. 277, 25 de noviembre de 1999.

[33] Herrán Ortiz, Ana I., *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales, op. cit.,* pp. 210-211.

1.1. El principio de calidad de los datos

Tal y como dispone la LOPD los datos personales «sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido»(art. 4.1 LOPD).

El principio de calidad de los datos legitima el tratamiento y ha de contemplarse desde una doble perspectiva: la cualidad del dato personal y la finalidad del tratamiento. Los datos pueden ser objeto de tratamiento porque se adecuan y respetan las finalidades legítimas de aquél; por lo que el dato será adecuado cuando esté directamente relacionado con la finalidad concreta que justifica el tratamiento; pero, también será adecuado, cuando responda con veracidad y exactitud a la situación real de la persona; y por otra parte, el dato personal no será excesivo si es necesario y proporcionado en relación con dicha finalidad, recordar en este sentido que en los debates previos a la aprobación de la Ley se hizo referencia a la necesidad de que los datos fueran «estrictamente indispensables»[34]. Es por ello que los datos personales deberán cancelarse cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados; y, no serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para el cumplimiento de los fines para los que hubieran sido recabados (art. 4.5 LOPD).

Por otra parte, además de exigirse que las finalidades sean «determinadas, explícitas y legítimas», prohibe la Ley la utilización de datos personales para «finalidades incompatibles» con aquellas para las que los datos hubieran sido recogidos. Y es en este punto donde los grupos Parlamentarios se mostraron especialmente críticos con la Ley, por considerar que como consecuencia de esta norma se producía una merma en las garantías de los ciudadanos. Abundando en lo expresado, se objeta a la norma que no se ajuste en sus previsiones a los dictados comunitarios, por cuanto que la Directiva 95/46/CE se refiere a «tratamiento incompatible», en tanto que el texto español alude a «finalidades incompatibles», lo que a juicio de algunos Grupos Parlamentarios no significa lo mismo, y en todo caso, parece que incluso podría vulnerar el principio de pertinencia de los datos[35].

---

[34] Cfr. Diario de sesiones del Congreso de los Diputados. Comisión Constitucional, VI Legislatura, sess. núm. 24, núm. 744, 15 de setiembre de 1999, p. 21884.

[35] Cfr. Diario de sesiones del Congreso de los Diputados.Comisión Constitucional, sess. núm. 24, VI Legislatura, núm. 744, 15 de septiembre de 1999, pp. 21867 y 21888.

Pero además, el principio de calidad de los datos exige que éstos sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado; si los datos personales resultaran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que tengan reconocidas los afectados. En efecto, el tratamiento de datos personales se justifica cuando la información tratada responde con veracidad y exactitud a la situación real y actual del interesado, en otro caso, el dato no será adecuado, ni pertinente, han de exceptuarse de esta obligación los supuestos en que el tratamiento se justifique por motivos históricos, estadísticos y científicos, en cuyo caso reglamentariamente se determinará el procedimiento por el cual se decida el mantenimiento íntegro de determinados datos.

1.2. El principio de transparencia del tratamiento

La protección de datos como sistema preventivo precisa que el legislador establezca la obligación de publicidad del tratamiento, de suerte que el interesado pueda conocer las circunstancias en que tiene lugar el tratamiento de sus datos, y pueda ejercitar eficazmente los derechos que el ordenamiento le reconoce. Por ello, el art. 5.1 de la LOPD establece que los interesados a los que se soliciten datos personales deberán ser previamente informados de forma expresa, precisa e inequívoca:

a) De la existencia de un fichero o tratamiento de datos personales, de la finalidad de la recogida de éstos y de los destinatarios de la información;
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas planteadas;
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
e) De la identidad y dirección del responsable del tratamiento o de su representante.

Ello no obstante, contempla la norma importantes excepciones al principio general de publicidad del tratamiento; así, si bien cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos en forma claramente legible, las advertencias del art. 5.1, no será necesaria la información de los apartados b), c) y d) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. No

puede desconocerse que esta exigencia presenta un importante avance en la tutela de los derechos, por cuanto que garantiza al afectado el derecho a conocer la existencia del tratamiento, los posibles derechos a ejercitar, así como la identidad del responsable del fichero; sin esta información no sería posible la tutela y ejercicio de los demás derechos reconocidos al interesado.

Asimismo, cuando los datos personales no se recaban del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero dentro de los tres meses siguientes al momento del registro de los datos, salvo que hubiera sido informado antes de la existencia y contenido del tratamiento, del origen de los datos, de la posibilidad de ejercitar sus derechos, así como de la identidad y dirección del responsable del tratamiento[36].

Claro que la LOPD introduce también importantes excepciones al principio general de información al interesado; por lo que cuando una ley expresamente lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de protección de datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a posibles medidas compensatorias, no será necesario cumplir con la obligación de información al interesado. Tampoco corresponderá informar al interesado cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos, de la identidad del responsable del tratamiento, y de los derechos que le asisten (art. 5.5. LOPD).

Puede objetarse a esta última excepción que no reproduzca fielmente las garantías y supuestos especiales que la Directiva 95/46/CE contempla; en efecto, la Directiva prevé la exclusión del derecho de información «en particular para el tratamiento con fines estadísticos, o de investigación histórica o científica, cuando la información al interesado

---

[36] Especialmente intensos fueron los debates a propósito de esta disposición, y así, se objeta al texto español su falta de sintonía con lo establecido en la norma comunitaria. La Directiva 95/46/CE establece en su art. 11 que los Estados miembros dispongan que el responsable del tratamiento deberá informar «desde el momento del registro de los datos, o en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos…». De ahí que se indicara la necesidad de que se informara en el mismo momento del registro o en la primera utilización, pero no tres meses después, por la inseguridad que esta demora provocaría. Cfr. Diario de sesiones del Congreso de los Diputados. Comisión constitucional, VI Legislatura, núm. 744, de 15 de septiembre de 1999, p. 21872.

resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por la ley», esto es, la exclusión se contempla únicamente para tales tratamientos cuando concurran las condiciones que la norma contempla; por el contrario, la LOPD amplía los supuestos, ya que además de a los tratamientos con fines científicos, históricos o estadísticos la excepción comprende aquellos otros que, a discreción de la Agencia de Protección de Datos, cumplan las condiciones descritas en el art. 5.5. de la LOPD.

Por último, debe advertirse que a propósito de la excepción contemplada al derecho de información para el caso de que los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección, nada establece la Directiva, con lo que el legislador español nuevamente va más allá de lo establecido en el texto comunitario, con el consiguiente menoscabo para los derechos y garantías de los interesados.

1.3. La necesidad del consentimiento informado

El principio del consentimiento en el derecho de protección de datos representa una condición indisponible sobre la que se fundamenta la licitud del tratamiento de datos y su legitimidad. Así, con carácter general reconoce el art. 6 de la LOPD que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa, bien entendido que el consentimiento podrá revocarse cuando exista causa justificada para ello, si bien no tendrá efectos retroactivos. Y así, dispone la LOPD que no será necesario el consentimiento cuando:

a) los datos personales se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias;
b) se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;
c) el tratamiento tenga por finalidad la protección del interés vital del interesado según el art. 7.6 LOPD;
d) los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Sorprende lo numeroso de las excepciones, y la utilización de conceptos jurídicos indeterminados, que no hacen sino contribuir a la inse-

guridad jurídica, objeción ésta que puede hacerse extensiva a la totalidad del texto. Así, por ejemplo, el concepto «interés vital del interesado» ofrecía importantes dificultades para su definición, tal y como se manifestó en los debates parlamentarios, en los que se cuestionaba el significado de este concepto[37], que finalmente se define en el art. 7.6 como aquellos tratamientos en los que resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que el tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta por igual obligación y también cuando el afectado esté físicamente o jurídicamente incapacitado para dar su consentimiento.

1.3.1. El derecho de oposición al tratamiento

El reconocimiento del derecho de oposición en la Directiva 95/46/CE facilitó su incorporación al texto español; de suerte que si bien no puede decirse que la LOPD siga fielmente en este punto las previsiones comunitarias al menos puede asegurarse que su configuración contribuye a reforzar los fundamentos de la protección de datos en el ordenamiento español. En efecto, si la Directiva 95/46/CE delimita los supuestos en los que será posible oponerse al tratamiento de datos, la LOPD opta por establecer un derecho de oposición general, para aquellos supuestos en los que no sea necesario el consentimiento, a no ser que una Ley excluya este derecho. Sin embargo, parece más rigurosa la LOPD al exigir para ejercitar la oposición que existan motivos fundados y legítimos relativos a una concreta situación personal, en tanto que la Directiva reconoce el derecho de oposición «en cualquier tiempo, por razones legítimas propias de su situación particular».

1.3.2. Los datos personales especialmente protegidos

Existe información relativa a la persona que por su proximidad a la esencia del individuo y por la vinculación con sus aspectos más interiores merece una protección reforzada. Así lo han entendido también los legisladores europeos que unánimemente han establecido normas

---

[37] «[…] ¿Qué es el interés vital? Nadie lo sabe… Nosotros entendemos que es la defensa básica de la vida y de la integridad física de las personas. Es un concepto fundamental como excepción al principio del consentimiento». Cfr. Diario de sesiones del Congreso de los Diputados. Comisión constitucional, VI Legislatura, núm. 744, 15 de septiembre de 1999, p. 21888.

especiales de tutela para la regulación del tratamiento de los datos denominados sensibles. Claro que no deben identificarse estos datos personales sensibles con datos relativos a la intimidad de las personas, bien al contrario, en ocasiones se trata de datos personales que hacen referencia a aspectos fácilmente apreciables de la persona, pero que por su trascendencia para el desarrollo individual precisan de una especial protección jurídica.

La LOPD ha establecido un régimen jurídico diferenciado, y al reconocer diferentes categorías de datos sensibles, ha configurado un sistema gradual de protección de los datos sensibles. Por ello, respecto a los datos relativos a la ideología, religión o creencias, proclama el art. 7.1 que nadie podrá ser obligado a declarar sobre ello; si bien cuando se proceda a recabar el consentimiento para el tratamiento de estos datos se deberá advertir al interesado acerca de su derecho a no prestarlo. Numerosas han sido las críticas que ha merecido esta norma, orientadas fundamentalmente a exigir unas previsiones más respetuosas y fieles con el texto constitucional que prohibe cualquier requerimiento de tales datos personales (art. 16.2 CE)[38]. Por tanto, el tratamiento de los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, sólo será legítimo con el consentimiento expreso y por escrito del afectado. Ello no obstante, se exceptúan los ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. Claro que, particularmente polémica resultó la exclusión de los ficheros de Iglesias, confesiones y comunidades religiosas en lo referente a sus asociados y miembros, por la dificultad para establecer quién sea miembro de una iglesia o confesión.

Por otra parte, los datos personales que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Los datos relativos a la salud tienen una especial relevancia porque están directamente vinculados al desarrollo físico de la persona; pero, también tienen significación especial

---

[38] «[…] requerir que alguien hable sobre su ideología, religión o creencias, sinceramente no encontramos nunca justificación de ello porque no son datos precisos para la convivencia ni para la relación humana, deben pertenecer a una esfera de tal intimidad que sólo requerir es ofensivo». Cfr. Diario de sesiones del Congreso de los Diputados. Comisión constitucional, VI Legislatura, núm. 744, 15 de septiembre de 1999, p. 21885.

para la Administración por su trascendencia para la gestión y prevención sanitaria. En este sentido, la Ley 41/2002, de 14 de noviembre, establece con carácter general el derecho de la persona a que se respete el carácter confidencial de los datos referentes a la salud, y a que nadie pueda acceder a ellos sin previa autorización legal; a estos efectos, los centros sanitarios adoptarán cuantas medidas sean necesarias para garantizar este derecho, y elaborarán cuando proceda normas y procedimientos protocolizados para garantizar el acceso legal a los datos de los pacientes[39]. Asimismo, y sin perjuicio de lo establecido para la cesión, las instituciones y centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de datos personales relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos (art. 14 Ley 41/2002, de 14 de noviembre).

Se prohiben con carácter general los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual (art. 7.4. LOPD).

Finalmente, los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Sorprende que el texto español, no siga en este punto las previsiones comunitarias, de suerte que sólo exige que la titularidad del fichero sea pública, pero no requiere que también sea la administración pública quien controle o gestione los ficheros. Asimismo, si la Directiva se refiere a los datos de «procesos civiles» nada establece a este respecto la LOPD.

Excepcionalmente, los datos personales de los apartados 2 y 3 del art. 7 podrán ser objeto de tratamiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por

---

[39] Recoge el Capítulo V de la citada norma la regulación de la denominada historia clínica, que comprende el conjunto de documentos relativos a los procesos asistenciales del paciente, con identificación de los médicos y demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, investigación o docencia se regirá por lo dispuesto en la LOPD y en la Ley 14/1986, General de Sanidad. Cfr. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, BOE núm. 274, de 15 de noviembre de 2002.

otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento estos mismos datos cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Significar que en principio se permitía el tratamiento «disociado» de tales datos —así se hacía constar en el dictamen de la Comisión constitucional— sucede sin embargo, que desaparece del texto esta exigencia, lo que no parece razonable ya que se facilita el tratamiento de datos sensibles incluso con fines de gestión de servicios sanitarios[40].

1.3.3. El consentimiento en la cesión de los datos personales

La información que ha sido recabada por el responsable de un fichero, que ha comunicado al interesado su finalidad, identidad del responsable y tipo de datos personales tratados, puede ser comunicada a otro destinatario para su posterior tratamiento por otro responsable. Luego la información al interesado sobre la comunicación de tales datos personales y la conformidad de aquél con el nuevo tratamiento constituyen también una necesidad para legitimar el nuevo tratamiento (Sentencia de la Audiencia Nacional de 14 de abril de 2000).

El principio general establece la necesidad del consentimiento para la cesión de datos personales, y siempre que ésta sea además para el «cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario». La primera objeción que puede introducirse a esta norma se refiere a la inobservancia del principio de finalidad, ya que sólo se exige que la finalidad de la cesión respete las actividades de cedente y cesionario; pero no es éste el criterio adoptado por la Directiva 95/46/CE en su considerando 28, cuando expresamente indica que «los objetivos de los tratamientos posteriores no pueden ser incompatibles con los objetivos originalmente especificados», lo que garantizaría al afectado que en ningún caso la cesión responda a finalidades incompatibles con las que inicialmente permitieron la recogida y tratamiento de los datos. Ahora bien, no será preciso el consentimiento previo a la cesión cuando:

a) la cesión esté autorizada por ley;
b) se trate de datos recogidos de fuentes accesibles al público;

---

[40] Cfr. Boletín Oficial de las Cortes Generales, VI Legislatura, serie A, núm. 135-10, 24 de setiembre de 1999, p. 75.

c) el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. La cesión sólo será legítima cuando se limite a la finalidad que la justifique;
d) la cesión que deba efectuarse tenga por destinatario al Defensor del Pueblo, Ministerio Fiscal, o los jueces o tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas; tampoco cuando sean destinatarios instituciones autonómicas con funciones análogas al Defensor del Pueblo o Tribunal de Cuentas;
e) la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;
f) la cesión de datos personales relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos establecidos en la legislación sobre sanidad.

Mereció importantes críticas la excepción al principio del consentimiento en la cesión de datos procedentes de fuentes accesibles al público, por cuanto que se pensaba que el hecho de que los datos se encontraran en tales fuentes no justificaba por sí solo la cesión de datos sin consentimiento del interesado, como tampoco su recogida y tratamiento. Y en verdad que así debía ser, que los datos personales se encuentren registrados en fuentes accesibles al público no excluye la necesidad del consentimiento para su tratamiento, en otro caso se desconocería respecto de estos ficheros el ejercicio de los derechos reconocidos al interesado frente al tratamiento de sus datos personales. Hubiera sido acertado exigir que el responsable del fichero que cede los datos informara de ello a la Agencia de Protección de Datos, para asegurar al afectado la publicidad de dicha comunicación, y de las circunstancias que la rodean; lo que refuerza la tutela del interesado, que podrá conocer el origen de los datos insertos en ficheros cuando no han sido recabados directamente del interesado.

Por otra parte, y de acuerdo con el principio de transparencia, establece la LOPD que será nulo el consentimiento para la cesión de datos personales a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden ceder.

Finalmente, se exceptúa la aplicación de las normas previstas para la cesión de datos personales cuando la comunicación se efectúa pre-

vio procedimiento de disociación; en efecto, no podrá deducirse perjuicio para los afectados cuando los datos personales no aparecen asociados a la persona a quien conciernen. Ahora bien, no establece el legislador una garantía adicional, por lo que hubiera sido oportuno que se garantizase que en lo sucesivo, los datos cedidos de forma disociada, no podrán volver a tratarse asociados a su titular.

Proclama por su parte la LOPD que no se considerará cesión de datos el acceso de un tercero a la información cuando el mismo sea necesario para la prestación de un servicio al responsable del tratamiento (art. 12.1 LOPD). Así, la realización del tratamiento por cuenta de terceros se regulará por contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos según instrucciones del responsable del tratamiento, que no los utilizará con un fin distinto al que figure en dicho contrato, ni los cederá a otras personas, estipulando también las medidas de seguridad que el encargado deberá adoptar de acuerdo con la Ley.

Cumplida la prestación contractual, los datos personales se destruirán o deberán ser devueltos al responsable, igual que el soporte o los documentos en que conste algún dato de carácter personal objeto del tratamiento. Por tanto, ya no es posible, como sucedía en la LORTAD, que el encargado conserve los datos personales por un periodo de cinco años aun cuando medie autorización del responsable, para el caso de que «razonablemente se presuma la posibilidad de ulteriores encargos», y siempre que se observaran las debidas garantías —que en verdad nunca se definieron legalmente—. Cuando el encargado destine los datos a otra finalidad, los comunique o utilice incumpliendo el contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

1.4. El principio de seguridad de los datos

Los principios de protección de datos personales además de garantizar la licitud del tratamiento, también pueden referirse al control del tratamiento, y exigir del responsable y del encargado del mismo un comportamiento activo, para que desarrollen las garantías y medidas necesarias para la seguridad del tratamiento y de los datos objeto del mismo. Por ello, el responsable del fichero y en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su

alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (art. 9 LOPD).

Destaca especialmente respecto a la anterior legislación la referencia expresa al encargado del tratamiento, que deberá igualmente adoptar las medidas de seguridad oportunas; esta novedad resulta coherente con la configuración y trascendencia que la figura del encargado del tratamiento alcanza en la nueva LOPD.

Por otra parte, la LOPD prevé las medidas de seguridad no sólo en el ámbito de los tratamientos automatizados de datos, sino también respecto de los ficheros manuales, circunstancia que deberá desarrollarse reglamentariamente, porque el actual Reglamento de seguridad expresamente excluye de su ámbito de aplicación los ficheros manuales. Asimismo, advierte la LOPD que no se podrán registrar datos personales en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamientos, locales, equipos, sistemas y programas…

En otro orden de consideraciones, la aplicación de la LORTAD en lo relativo a las medidas de seguridad tropezó con la ausencia de un desarrollo reglamentario que estableciera las obligaciones del responsable del fichero en materia de seguridad, lo que en la práctica significó la ineficacia absoluta de este esencial principio de protección de datos. Así, se aprobó en 1999 el Reglamento de medidas de seguridad de los ficheros automatizados de datos personales, que continúa en vigor a la espera de un nuevo texto que desarrolle las exigencias de la actual legislación[41].

Coincidimos con MARTÍNEZ SÁNCHEZ en señalar que el Reglamento al establecer tres niveles de seguridad, (básico, medio y alto), ha pretendido crear un marco general para facilitar la elaboración de medidas de seguridad que refuercen las garantías del tratamiento, al tiempo que establece un nivel de seguridad adecuado para favorecer el equilibrio entre los riesgos, los conocimientos técnicos existentes y el coste de aplicación de las medidas[42].

---

[41] Cfr. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, BOE núm. 151, de 25 de junio de 1999.

[42] MARTÍNEZ SÁNCHEZ, Mar, «Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal», *Actualidad Jurídica Aranzadi,* núm. 35, 2000.

Los niveles de seguridad que establece el Reglamento se disponen atendiendo a la naturaleza de los datos tratados, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, y así según dispone el Reglamento:

a) todos los ficheros de datos personales adoptarán medidas de seguridad de nivel básico;
b) los ficheros de datos sobre comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, y de prestación de servicios de información sobre solvencia patrimonial y crédito, adoptarán las medidas de nivel básico y medio;
c) los ficheros de datos sobre ideología, religión, creencias, origen racial, salud, o vida sexual, o los que tengan datos recabados con fines policiales sin consentimiento del interesado deberán además de las anteriores adoptar las medidas de nivel alto;
d) los ficheros que contengan datos personales suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar además de las medidas de nivel básico las de nivel medio.

Establecen con acierto Del Peso y Ramos González una clasificación de los controles a establecer, de suerte que se refieren a: controles directivos, que son los que establecen las bases o políticas de protección; controles de naturaleza preventiva, para evitar problemas derivados de intervenciones de terceros; controles correctivos, previstos para rectificar errores, negligencias o actuaciones malintencionadas y controles de recuperación, que preparan y permiten la restauración de la situación anterior a la intrusión o accidente[43].

Las medidas de seguridad previstas en el Reglamento consisten[44]:

a) El documento de seguridad, de obligado cumplimiento para el personal con acceso a los datos personales automatizados y a los sistemas de información;
b) Control del personal con acceso a los datos personales y a los sistemas, que tendrá definidas sus funciones y obligaciones;
c) Registro de incidencias, para hacer constar todas las incidencias, y las circunstancias en que se conocen y comunican;

---

[43] Del Peso Navarro, Emilio y Ramos González, Miguel A., *La seguridad de los datos de carácter personal,* Madrid, Díaz de Santos/IEE, 2002, pp. 6-7.

[44] Para profundizar en esta cuestión Del Peso Navarro, Emilio y Ramos González, Miguel A., *La seguridad de los datos de carácter personal,* Madrid, Díaz de Santos/IEE, 2002.

d) Identificación y autentificación, estableciendo una relación actualizada de usuarios que tengan acceso autorizado al sistema de información;
e) Control de acceso, adoptando medidas para impedir el acceso a datos o recursos a un usuario no autorizado;
f) Gestión de los soportes, que cuando contengan datos personales permitirán identificar el tipo de información, y serán inventariados y conservados en lugar de acceso restringido;
g) Copias de respaldo y recuperación, deberán realizarse al menos semanalmente;
h) Auditoria, propia de las medidas de seguridad de nivel medio, para garantizar que los sistemas de información e instalaciones de tratamiento de datos se someten a una auditoría interna o externa, que verifique el cumplimiento del Reglamento y de las instrucciones sobre seguridad de los datos, al menos cada dos años.

Ahora bien, puede objetarse al Reglamento que únicamente alcance a aplicarse a los ficheros de datos personales, automatizados, por lo que los convencionales quedan al margen de su regulación; y por otra parte, el Reglamento se configura como norma de mínimos, de forma que establece las medidas de seguridad básicas a cumplir por todos los ficheros de datos personales, sin perjuicio de las particulares medidas de seguridad que proceda adoptar cuando se trate de ficheros de características especiales.

Por último, la confidencialidad de los datos personales constituye otra importante medida de seguridad, que garantiza el respeto a la intimidad de los ciudadanos, por ello establece la LOPD que el responsable del fichero, y todos aquellos que intervengan en cualquier fase del tratamiento, deberán guardar secreto profesional, obligación que subsiste aun después de finalizar sus relaciones con el titular o el responsable del fichero. Obsérvese que la LOPD reserva la calificación de infracción muy grave para la vulneración de la confidencialidad de los datos sensibles del art. 7 y de los datos con fines policiales recabados sin consentimiento; en tanto que la infracción será grave cuando se trate de datos relativos a la comisión de infracciones administrativas y penales, Hacienda pública, servicios financieros, solvencia patrimonial y crédito y aquellos que permitan evaluar la personalidad del individuo (art. 44.3 LOPD). Llama la atención que la vulneración del deber de confidencialidad de datos relativos a infracciones penales no merezca para el legislador una mayor sanción, habida cuenta de la importancia social de tales datos, y de la necesidad del individuo de reinsertarse plenamente en la sociedad, para alcanzar su pleno desarrollo personal, familiar y laboral.

2. *Los derechos de las personas y la protección de datos*

Los principios de protección de datos hasta ahora estudiados necesitan hacerse efectivos, de suerte que no queden reducidos a meras normas o criterios programáticos; por ello, se configuran y alcanzan efectividad práctica a través del reconocimiento de los derechos y garantías individuales de protección de datos, que constituyen los instrumentos jurídicos en defensa de los intereses de los afectados en el tratamiento de sus datos personales.

Ahora bien, los derechos que integran el contenido esencial de la protección de datos son independientes, y el ejercicio de ninguno de ellos es requisito previo para el ejercicio de otro derecho (Norma Segunda Instrucción 1/1998 de la Agencia de Protección de Datos)[45].

2.1. El derecho de impugnación de valoraciones basadas exclusivamente en tratamientos automatizados

Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base exclusivamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad (art. 13 LOPD).

No pueden ignorarse las importantes diferencias que separan a la regulación de la LOPD del texto comunitario. En principio, la Directiva 95/46/CE se refiere a decisiones y valoraciones basadas exclusivamente en un «tratamiento automatizado» de datos, en tanto que la LOPD no introduce esta matización, al referirse a todo tratamiento de datos. Lo cierto es que esta omisión no parece casual, sino que es fruto del excesivo celo del legislador español por desterrar cualquier referencia legal al tratamiento automatizado de datos personales. Por otra parte, si la Directiva se refiere al derecho de las personas a no verse sometidas a tales decisiones cuando les perjudiquen, la LOPD reconoce el derecho a los «ciudadanos». Cierto es sin embargo, que esta norma ha de matizarse a tenor de lo establecido en el art. 1 de la LOPD

[45] Cfr. Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, sobre el ejercicio de los derechos de acceso, rectificación y cancelación, BOE núm. 232, de 29 de enero de 1998.

que expresamente declara como objeto de su regulación la protección de los derechos y libertades públicas de las personas físicas. Asimismo, a diferencia de la Directiva, la LOPD no define los aspectos de la personalidad a evaluar en los tratamientos automatizados que funden las decisiones, y en este punto, ha de felicitarse al legislador por esta omisión, ya que no se restringe el derecho de impugnación a los supuestos enunciados legalmente.

Ha merecido especiales críticas el apartado 3 del art. 13 de la LOPD cuando establece que «en este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto». Piénsese que el derecho a la información no puede quedar reducido a meros criterios o programas, se deberá ofrecer al interesado información completa de las bases sobre las que se ha sustentado la decisión que le perjudica porque sólo así podrá hacerse efectivo el derecho.

Y concluye el legislador indicando que «la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado».

2.2. Los derechos de consulta y acceso a la información personal

Reconoce la LOPD un derecho de consulta general, por el cual cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos personales, sus finalidades y la identidad del responsable del tratamiento (art. 14 LOPD). Por un lado, se reconoce el derecho de consulta a «cualquier persona», no al interesado, ya que la información que se facilita no afecta de forma individual al interesado. Por otro lado, el reconocimiento de este derecho constituye una pieza clave en el sistema de protección de datos, por cuanto que permite el posterior ejercicio del derecho de acceso por el interesado, ante el responsable del tratamiento, ello no obstante, hay que subrayar que resulta extremadamente restringido el objeto de la consulta.

El derecho de acceso, también conocido como *habeas data*, reconoce al interesado «el derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos» (art. 15.1 LOPD). Garantiza este derecho que el interesado conozca los datos objeto de tratamiento, y el origen de los mismos, así como posibles cesiones, de suerte que pueda valorar si el tratamiento es lícito, y respeta todos los principios de protección de datos.

La Instrucción 1/1998 de la Agencia de Protección de Datos al regular el ejercicio de los derechos de protección de datos indica que se trata de un derecho personalísimo, a ejercitar por el afectado, frente al responsable del fichero, si bien aquél podrá actuar mediante representante legal cuando se encuentre en situación de incapacidad o minoría de edad. El derecho de acceso podrá ejercitarse, conforme permite la técnica actual, mediante la consulta de los datos por visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos; bien entendido, que además, tal y como establece el art. 12.2 del RD 1332/94, de 20 de junio se admitirá también «cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del fichero»[46].

La petición de acceso deberá resolverse en el plazo de un mes a contar desde la recepción de la solicitud, transcurrido dicho plazo sin que se reciba respuesta, se entenderá que la petición se ha desestimado; si fuera estimada, el acceso se ejercitará en los diez días siguientes a la notificación de la resolución estimatoria (art. 12.3 RD 1332/94). Ahora bien, ni el Convenio 108 del Consejo de Europa, ni la Directiva 95/46/CE, establecían un plazo para el ejercicio de este derecho, pero la LOPD advierte que el derecho de acceso sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Excepcionalmente el derecho de acceso podrá denegarse cuando:

a) del acceso a ficheros de las Fuerzas y Cuerpos de Seguridad con fines policiales, de una investigación concreta pudieran derivarse peligros para la defensa del Estado, o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de investigaciones en curso;
b) se trate de ficheros de Hacienda Pública si el acceso obstaculiza las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias, y en todo caso, cuando el afectado esté siendo objeto de inspección;

---

[46] Cfr. Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, BOE núm. 147, de 21 de junio de 1994. Declarado en vigor por la Disposición Transitoria Tercera de la LOPD en cuanto no se oponga a lo establecido en la citada norma.

c) el derecho de acceso tenga que ceder ante razones de interés público o ante intereses de terceros más dignos de protección;
d) el acceso sea solicitado por persona distinta al afectado en el caso de ficheros de datos de titularidad privada.

Si bien el Convenio 108 del Consejo de Europa y la Directiva 95/46/CE prevén la posibilidad de ejercitar el acceso a los datos «sin gastos excesivos», la LOPD reconoce el derecho a obtener información de los datos de forma gratuita, por lo que se facilita el ejercicio de este derecho, al asegurar que la exigencia de una contraprestación en ningún caso constituirá un freno para el ejercicio de este derecho por los interesados[47].

2.3. Los derechos de rectificación, cancelación y bloqueo de los datos

El interesado ya ha consultado el Registro General de Protección de Datos, y después ha podido acceder a la información relativa a sus datos personales objeto de tratamiento, y es en este momento cuando se han establecido las condiciones mínimas y necesarias para el cumplimiento de los derechos de rectificación, bloqueo y cancelación de los datos.

Y así, tal y como establece el art. 16.2 de la LOPD los datos personales serán rectificados o cancelados, en su caso, cuando el tratamiento no se ajuste a lo dispuesto en la LOPD, y en particular, cuando tales datos resulten inexactos o incompletos. Abundando en lo expresado, coincidimos con Pérez de Velasco en afirmar que la rectificación y la cancelación constituyen dos derechos diferentes; procederá rectificar los datos cuando éstos sean erróneos o inexactos, y se cancelarán cuando sean inadecuados o excesivos en relación con la finalidad del tratamiento, así como cuando se produzca la revocación del consentimiento prestado. Rectificar no significa borrar o destruir físicamente la información, sino la sustitución de datos personales inexactos o incorrectos por otros actuales y correctos, pero siempre que no exista desviación del fin, o un uso desproporcionado de los mismos[48].

En la actualidad, el responsable rectificará o cancelará los datos personales en el plazo de diez días, recordar que según el art. 15.2 del

---

[47] El art. 12.1 de la Directiva 95/46/E y el art. 8.b) del Convenio 108 del Consejo de Europa garantizan al interesado el derecho de acceso sin gastos excesivos; lo que significa que como normas de mínimos facultan a los Estados para que puedan establecer una contraprestación para el derecho de acceso, si bien en ningún caso dicha carga podrá representar en la práctica un obstáculo que dificulte o impida el ejercicio del acceso.

[48] Pérez de Velasco, José Ramón, «Protección de datos de carácter personal», *Revista Electrónica de Derecho Informático,* núm. 27, 2000.

RD 1332/94 estos derechos se hacían efectivos en el plazo de los cinco días siguientes a la recepción de la solicitud.

La cancelación decía el art. 15.4 de la LORTAD «no procederá cuando pudiese causar un perjuicio a los intereses legítimos del afectado o de terceros o cuando exista una obligación de conservar los datos», esta excepción que desaparece del nuevo texto de la LOPD, se mantiene en la Norma Tercera apartado 5 Instrucción 1/1998, si bien entendemos que como excepción desaparece por cuanto que la nueva regulación no la contempla explícitamente, como sí hacía la LORTAD, por lo que puede interpretarse que es voluntad del legislador que no se aplique. Asimismo, los datos personales deberán conservarse durante los plazos previstos en las disposiciones aplicables, o en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado (art. 16.5 LOPD).

Cuando los datos personales que deban rectificarse o cancelarse hayan sido objeto de cesión, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, para que proceda también a su cancelación, en el art. 12.c) de la Directiva 95/467CE la obligación de notificación se amplía explícitamente al derecho de bloqueo, por lo que habrá que entender que también cuando proceda el bloqueo de los datos el cesionario deberá ser informado.

Por su parte, el art. 16.3 de la LOPD reconoce que «la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión». La novedad se encuentra en que la LORTAD no reconocía este derecho, si bien el posterior desarrollo reglamentario regulaba el derecho de bloqueo en el RD 1332/94, que en su art. 16 restringía el bloqueo a aquellos supuestos «en que siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado», con el fin de impedir su posterior proceso de utilización. Claro que a tenor de lo dispuesto en la Norma Tercera de la Instrucción 1/1998 no será posible el bloqueo cuando «se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en que figuren».

Las actuaciones contrarias al reconocimiento de estos derechos podrán ser objeto de reclamación ante la Agencia de Protección de Datos, según la forma en que reglamentariamente se determine; se procede

de esta manera a una desjudicialización de estas reclamaciones, lo que en modo alguno imposibilitará el acceso a la jurisdicción ordinaria. Por otra parte, la LOPD reconoce a quien se deniegue el ejercicio de los derechos de oposición, acceso, cancelación o rectificación la «facultad de ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación» (art. 18.2 LOPD). Se atribuye a la Agencia de Protección de Datos una facultad de control sobre el ejercicio de los derechos de los interesados, si bien en la práctica no tiene otra trascendencia que la mera verificación, ya que nada se establece a propósito de los efectos de este control, o de la facultad de la Agencia para requerir del responsable el cumplimiento de las previsiones legales. Habrá que esperar al desarrollo reglamentario, y confiar en que se reconozca a la Agencia el protagonismo que merece en la defensa del derecho a la protección de datos.

2.4. El derecho a la indemnización

Quien cause daño a otro debe indemnizar por ello, según una máxima del Derecho civil, y en verdad que en sí misma la actividad de tratamiento de datos implica potencialmente un conjunto de riesgos y amenazas para los derechos y libertades individuales que hacen necesario establecer un régimen de responsabilidad por el tratamiento de datos personales.

Por ello, y por la especial amenaza que el tratamiento de datos representa reconoce la LOPD que «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados» (art. 19.1 LOPD). Ahora bien, se mantiene la dualidad en el régimen de responsabilidad entre los ficheros públicos y privados, y así, «cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria»(art. 19.2 y 3 LOPD).

Recapitulando, se hace depender el régimen de responsabilidad civil del incumplimiento de las normas por el responsable del tratamiento, y no se vincula el deber de reparar el daño con la existencia del tratamiento; por ello, no será suficiente la relación de causalidad entre el tratamiento de datos y el perjuicio, se precisa además que pueda im-

putarse al responsable del tratamiento un incumplimiento del que se derive el daño[49].

Ha debatido la doctrina también ampliamente a propósito de la culpa exclusiva del afectado como causa de exclusión de la responsabilidad, y hay que recordar a este respecto que si bien nada se prevé en la LOPD, así se establece en la Directiva 95/46/CE, por lo que la culpa exclusiva del interesado también impide que pueda imputarse al responsable del tratamiento el deber de reparar el daño.

Para finalizar, debe reprocharse al legislador español que sean numerosos e importantes los silencios legales en materia de responsabilidad por el tratamiento de datos; así, quedan sin respuesta en la LOPD cuestiones como los perjuicios a que se extiende la indemnización, la forma en que han de valorarse los daños y las excepciones a la responsabilidad legal.

En primer lugar, de excluir el daño moral, tal como proponen algunos autores, poco será lo que quede para indemnizar; surge, también la duda respecto a la valoración misma de este daño, a la que la Ley tampoco ofrece respuesta. Ahora bien, en cada caso tendrán que valorarse aspectos tales como la naturaleza de los derechos implicados, la difusión concedida a tales datos y el lucro o beneficio obtenido con el tratamiento. No compartimos en este punto las afirmaciones de Ortí Vallejo por las cuales no ha de admitirse judicialmente con carácter general el reconocimiento de indemnizaciones por la utilización indebida de los medios informáticos, ya que ello impediría —a su juicio— una deseable despatrimonialización de los derechos fundamentales[50]. Desde luego, constituye un error enfrentar la despatrimonialización de los derechos fundamentales al reconocimiento de un legítimo derecho a recibir indemnización por los daños y perjuicios que a los bienes y derechos personales haya causado el tratamiento de datos personales[51].

---

[49] Así lo ha interpretado Grimalt Servera al considerar que se excluye la existencia de una responsabilidad objetiva absoluta, porque se configura un régimen de imputación a partir del incumplimiento de los deberes u obligaciones legales del responsable del tratamiento; por ello, si ha existido incumplimiento, y de éste se deriva un perjuicio para el afectado tendrá derecho a indemnización, con independencia de la concurrencia o no de culpa. Cfr. Grimalt Servera, Pedro, *La responsabilidad civil en el tratamiento automatizado de datos personales,* Colecc. Estudios de Derecho Privado, núm. 8, Granada, Comares, 1999.

[50] Ortí Vallejo, Antonio, *Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada, op. cit.,* pp. 168-169.

[51] Herrán Ortiz, Ana Isabel, *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*, *op. cit.,* p. 260.

En efecto, no puede desconocerse el derecho de indemnización del daño moral porque el interesado tenga reconocidos otros derechos de defensa frente al tratamiento de sus datos, como el derecho de oposición, rectificación o cancelación de los datos. Se trata de derechos diferentes, unos intentan prevenir utilizaciones ilícitas de los datos, y el otro pretende resarcir un incumplimiento del que se ha derivado un perjuicio para el interesado.

Por último, respecto a las causas de exención de responsabilidad, además de las señaladas, serán de aplicación las previstas en la Directiva, y también otras como la intervención exclusiva de un tercero, el ejercicio legítimo de un derecho, el estado de necesidad o el consentimiento de la víctima.

3. *Los tratamientos de datos personales en la Ley Orgánica 15/99. Especial referencia a los ficheros de titularidad pública*

Si la Directiva 95/46/CE no establece un marco jurídico diferenciado para la regulación de los ficheros públicos y privados, la LOPD establece regímenes jurídicos diferentes para el tratamiento de datos en el sector privado y en el ámbito de las Administraciones públicas. Y en verdad no han faltado autores críticos con esta decisión del legislador español, por entender que: por un lado, no se ajustaba al Derecho comunitario, que demanda un tratamiento unitario de todos los ficheros de datos personales; y por otro lado, porque esta dicotomía constituye un medio para privilegiar arbitrariamente a los ficheros de titularidad pública[52].

3.1. Su creación, modificación y supresión

Acoge la LOPD un régimen formal de regulación de los ficheros públicos, por cuanto que establece que la creación, modificación o supresión de estos ficheros sólo podrá hacerse por medio de disposición general publicada en el BOE o Diario oficial correspondiente (art. 20.1 LOPD). Si bien no ha de interpretarse que necesariamente ha de ser una Ley en sentido formal la que establezca la creación del fichero público, lo

---

[52] Cfr. Heredero Higueras, Manuel, «La transposición de la Directiva 95/46/CE en el Derecho positivo español», *X Encuentros sobre Informática y Derecho,* Universidad Pontificia Comillas, Instituto de Informática Jurídica, Madrid, 1997, p. 139. Alonso Blas, Diana, «La aplicación de la Directiva Europea de protección de datos en España», *X Encuentros sobre Informática y Derecho,* Universidad Pontificia Comillas, Instituto de Informática Jurídica, Madrid, 1997, p. 147.

cierto es que la constitución y el posterior funcionamiento de estos ficheros se encuentra condicionado por dos circunstancias: primera, la potestad reglamentaria de las Administraciones públicas deberá ejercitarse conforme a las disposiciones legales; y segunda, la habilitación legal para la creación de los ficheros públicos tiene su origen en la Ley, por lo que será preciso amparo legal para la creación por las Administraciones de sus ficheros. Ello no obstante, no puede ignorarse que estas disposiciones generales de creación de los ficheros además de normas de organización administrativa, desarrollan la LOPD e inciden en los derechos y libertades de la persona, con lo que sería aconsejable que tuvieran rango de Ley, o en su caso, habilitación legal expresa.

Por otra parte, será necesario notificar a la Agencia su existencia, para proceder de oficio a la inscripción de los ficheros públicos en el Registro General de Protección de Datos (art. 39.2.a) LOPD), y se deberá recabar de la Agencia de Protección de Datos el preceptivo informe, como corresponde respecto a los proyectos de disposiciones generales que desarrollen la Ley, tal como es el caso de las disposiciones de creación de ficheros públicos (art. 37. h LOPD).

La disposición normativa de creación o modificación del fichero público indicará las siguientes circunstancias:

a) finalidad y usos previstos para el fichero
b) personas o colectivos sobre los que se pretenda recabar información o que resulten obligados a suministrarlos, y el procedimiento de recogida
c) estructura básica del fichero y descripción de los tipos de datos personales incluidos, así como las cesiones y transferencias de datos a países terceros
d) órganos de las Administraciones públicas responsables del fichero, y servicios ante quien ejercitar los derechos de acceso, rectificación, cancelación y oposición
e) las medidas de seguridad, con indicación del nivel exigible.

Respecto a la supresión de los ficheros públicos, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción (art. 20.3 LOPD). Así las cosas, para una correcta interpretación de esta disposición conviene precisar dos cuestiones: por un lado, qué entiende el legislador por «determinar el destino de los datos»; y por otro lado, qué significa destruir los ficheros.

La destrucción se equiparará a la desaparición física del fichero, a su supresión total y no sólo a su inutilización. Claro que admite también la norma una posibilidad diferente, cuando contempla la necesidad de que se informe del destino, por lo que se permite una próxima

recuperación de la información, siempre que el destino establecido haya sido el bloqueo o la inutilización.

3.2. La comunicación de datos entre Administraciones públicas

Tal y como apuntaba la Exposición de Motivos de la derogada LORTAD, el verdadero peligro del tratamiento de datos personales no se encuentra en el almacenamiento de los datos, sino en la cesión de la información a terceros, sin conocimiento del interesado. En la actualidad, los avances informáticos facilitan la creación de sistemas y redes de información a las que es sencillo acceder, para poder realizar un cruce de datos o una cesión no consentida. Una muestra de la inquietud y preocupación que la cesión de datos personales entre Administraciones públicas genera fueron los intensos debates parlamentarios que precedieron a la aprobación de la LOPD, en los que se llegó a tachar a la nueva Ley de «cheque en blanco» para las Administraciones, porque facilitaba una cesión de datos en masa y generalizada como consecuencia de las excepciones introducidas[53].

Como norma general establecía originariamente el art. 21.1 de la LOPD que «los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos». Por tanto, el principio general en la cesión de datos entre administraciones públicas es la autorización de su realización, y estará prohibida la comunicación cuando sean cedidos para el ejercicio de competencias diferentes o que versen sobre materias distintas. Incluso en estos últimos casos, la cesión era posible y lícita cuando estuviera prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Fueron numerosas las enmiendas al texto legal, y todo hacía presagiar que nuevamente, tal y como ya hiciera contra la LORTAD, el Defensor del Pueblo interpondría contra el art. 21.1 de la LOPD un nuevo recurso de

---

[53] Cfr. Diario de sesiones del Congreso de los Diputados. Comisión Constitucional, VI Legislatura, núm. 744, 15 de septiembre de 1999, p. 21868.

inconstitucionalidad. Y así fue, entiende el Defensor del Pueblo en su recurso que la nueva Ley incurre en los mismos errores que ya fueron denunciados en la anterior legislación, y en especial que «la posibilidad de ceder datos personales sin consentimiento del titular supone una limitación al derecho reconocido en el artículo 18.4 de la Constitución que sólo en supuestos tasados y debidamente justificados podría imponer una norma con rango de Ley. […] que el art. 21.2 contiene una remisión en blanco al Ejecutivo, incondicionada y carente de límites ciertos y estrictos, para fijar los casos en los que proceda autorizarse la cesión de datos entre administraciones públicas sin consentimiento del titular, contraria al principio de reserva de ley proclamado en el art. 53.1 de la Constitución». Finalmente, la STC 292/2000 ha declarado contrario a la Constitución y nulo el inciso del art. 21.1 LOPD «cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso»[54].

En todo caso, podrán ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra. Asimismo, para la cesión de datos obtenidos de fuentes accesibles al público, establece excepcionalmente el art. 21.3 LOPD que, no obstante lo establecido en el art. 11.2.b), la comunicación de tales datos no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa. De este modo, se respeta el principio del consentimiento, ya que si bien los datos han sido obtenidos de fuentes accesibles al público, ello no significará que los interesados no deben ser informados de las posibles cesiones de estos datos, y en su caso que no deban consentir dicha comunicación.

3.2. Los ficheros de las Fuerzas y Cuerpos de Seguridad

Mantienen como ficheros públicos un régimen jurídico especial los ficheros de las Fuerzas y Cuerpos de Seguridad (en adelante FFCCSS), si bien la Ley establece dos categorías de tratamientos: por un lado, los

---

[54] Ha declarado el TC que «la remisión a la regulación reglamentaria de materia ligada a la reserva de ley es preciso, pues, que se formule en condiciones tales que no contraríe materialmente la finalidad de la reserva […] la LOPD en este punto no ha fijado por sí misma, como le impone la Constitución (art. 53.1 CE), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 LOPD, en relación con lo dispuesto en los arts. 4, 6 y 34.e LOPD), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar». Cfr. STC 292/2000, de 30 de noviembre, BOE núm. 4, de 4 de enero de 2001.

relativos a fines administrativos, y por otro, los que cumplen una función estrictamente policial. Así, señala el art. 22.1 que los ficheros creados por las FFCCSS que contengan datos personales que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la LOPD. Sin embargo, la recogida y tratamiento de datos personales para fines policiales por las FFCCSS sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

En consecuencia, la definición de los fines de los ficheros policiales, y en concreto la determinación de qué se entiende por fines policiales constituye una cuestión de especial trascendencia para la regulación de estos ficheros; y así, siguiendo la definición prevista en la Recomendación n.º R (87) 15 se consideran fines policiales «el conjunto de tareas que incumbe a las autoridades policiales para la prevención y represión de las infracciones penales y el mantenimiento del orden público»[55]. Así, pues, los ficheros policiales fundamentan la especialidad de su regulación en la excepcionalidad de los fines del tratamiento, de suerte que podrán almacenarse y tratarse datos personales sin el consentimiento del afectado con fines policiales cuando «resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales», si bien cuando los datos personales se obtengan para fines distintos no será posible exceptuar la necesidad del consentimiento del interesado. Llama la atención la abusiva utilización de conceptos jurídicos indeterminados, que en nada favorecen una interpretación restrictiva de las excepciones al ejercicio de los derechos; en efecto, ¿Qué debe entenderse por peligro real? ¿Cuándo resultarán los datos necesarios? ¿Admite el legislador implícitamente la posibilidad de almacenar datos poco fiables? ¿Con qué garantías?

Asimismo, la recogida y tratamiento por las FFCCSS de los datos sensibles podrán realizarse «exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa

---

[55] La Recomendación n.º R (87) 15 adoptada por el Comité de Ministros del Consejo de Europa el 17 de septiembre de 1987 relativa a la protección de datos en el sector policial, ya apuntaba la necesidad de conciliar el respeto a los derechos individuales de los ciudadanos a su intimidad y vida privada con los intereses generales de prevención y represión de infracciones penales para el mantenimiento del orden público.

o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales» (art. 22.3 LOPD). Se ha acogido de forma positiva por la doctrina la introducción en la LOPD del control jurisdiccional sobre estos datos, ya que si bien pueden ser necesarios para una concreta investigación, deben estar sometidos a un especial control habida cuenta de la particular incidencia que alcanzan en la tutela de la persona; por ello, corresponderá a la autoridad judicial decidir sobre el carácter absolutamente necesario del tratamiento de los datos sensibles[56]. Sin embargo, no se encontró exenta de polémica la aprobación de esta disposición, a la que se enfrentaron numerosos Grupos Parlamentarios que entendían que no quedaban suficientemente garantizados los derechos individuales de los interesados, por lo que se proponía un control judicial previo del tratamiento, o en su caso, una previa comunicación a la Agencia de Protección de Datos[57].

Por otra parte, los ficheros de datos personales con fines policiales tienen carácter transitorio, por ello, «se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad» (art. 22.4 LOPD). Abundando en lo expresado, significar que con carácter general en aplicación del principio de finalidad del tratamiento, el art. 4.5. de la LOPD advierte que «los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados». La cancelación se producirá de oficio, por lo que el responsable del fichero deberá suprimir los datos cuando aprecie que no son precisos para los fines concretos de una investigación, porque no puede ignorarse que estos ficheros tienen carácter temporal.

Continuando con el excepcional régimen jurídico previsto en la LOPD para los ficheros policiales, el art. 23.1 faculta a los responsables de los ficheros de las FFCCSS para que puedan «denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran

---

[56] ALVAREZ-CIENFUEGOS SUÁREZ, José María, «Notas a la nueva regulación de la protección de datos de carácter personal (Ley orgánica 15/1999, de 13 de diciembre)», *La Ley,* núm. 3, 2000.

[57] Cfr. Diario de sesiones del Congreso de los Diputados. Comisión Constitucional, VI Legislatura, núm. 744, de 15 de septiembre de 1999, pp. 21875 y ss. a

derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando». Ninguna garantía adicional se contempla en la LOPD a propósito de estas excepciones, ya que si bien es cierto que encuentran amparo legal en el marco comunitario de la Directiva 95/46/CE (art. 10), no es menos cierto que la citada Directiva es norma de mínimos y nada hubiera impedido una protección más garantista de los derechos y libertades fundamentales en relación con el tratamiento de datos sensibles en el sector policial, y en lo referente al ejercicio de los derechos de protección de datos. Con razón y cierto desasosiego se advertía en los debates parlamentarios que el problema de los ataques a la intimidad a través de la informática es el desconocimiento del interesado, de ahí la necesidad de informar sobre la existencia de los ficheros, para evitar la indefensión de los interesados[58].

3.3. Excepciones y limitaciones al ejercicio de los derechos

Además de las particulares excepciones que la LOPD introduce en la regulación de los ficheros de las FFCCSS, prevé un régimen general privilegiado para los ficheros públicos, que ha sido calificado de «euforia de las excepciones», en clara referencia a los excesivos límites y restricciones que se introducen al ejercicio de los derechos de las personas.

A propósito de los ficheros de la Hacienda Pública ya ha tenido ocasión de manifestarse el TS, cuando ante un posible conflicto entre los intereses públicos en materia fiscal y el derecho a la intimidad ha subrayado que «es forzoso considerar que dicho derecho —a la intimidad— como los demás derechos fundamentales, no es ilimitado, sino que tiene su límite en la necesidad de proteger y preservar otros derechos fundamentales u otros bienes constitucionalmente protegidos. […] el deber de todos de contribuir al sostenimiento de las cargas públicas

[58] «[…] si las Fuerzas y Cuerpos de Seguridad del Estado dicen: no le digo a usted si está en mi fichero o no, no le permito que acceda ni que rectifique ni que cancele; aunque mis datos sean manifiestamente falsos no se lo permito, porque lo necesito para la investigación que estoy realizando, ¿qué va a decir la Agencia de Protección de Datos? Nada. ¿Qué es procedente o improcedente si la propia Ley está permitiendo que no se rectifique, que no se cancele, que no se acceda, en función de los peligros que pudieran derivarse para la defensa de la seguridad pública —un concepto tan amplio como la seguridad pública—, la protección de los derechos y libertades de terceros o las necesidades de la investigación? Es una cláusula enormemente abierta que, a nuestro juicio, vulnera el art. 18.4 de la Constitución sin ninguna concreción y que no tiene ningún control». Cfr. Diario de sesiones del Congreso de los Diputados. Comisión Constitucional, VI Legislatura, núm. 744, de 15 de septiembre de 1999, p. 21869.

de acuerdo con su capacidad económica, mediante un sistema tributario justo, que sanciona el art. 31.1 de la Constitución, constituye un bien constitucionalmente protegido para cuyo efectivo cumplimiento es evidentemente necesaria la inspección fiscal, y la injerencia que para el cumplimiento de ese deber pudiera producirse en el derecho a la intimidad no podría calificarse de arbitraria» (STS de 16 de abril de 1998).Y así, la LOPD en su art. 23.2 faculta a los responsables de los ficheros de la Hacienda Pública para denegar el ejercicio de los derechos de acceso, rectificación, o cancelación cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras. Así lo ha entendido también el TS cuando en su Sentencia de 5 de junio de 1995 rechaza que la denegación del acceso a los datos tributarios registrados en el Centro de procesos de datos constituya una vulneración del derecho a la intimidad, por cuanto que se trata —a juicio del Tribunal— de datos facilitados por terceros, relativos a operaciones y movimientos económicos del interesado, y por tanto, debe prevalecer el interés general materializado en la obligación constitucional de contribuir al sostenimiento de las cargas tributarias.

Por otra parte, trata la LOPD de establecer nuevas garantías en su art. 23.3 al reconocer que el afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, rectificación o cancelación «podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación». Obsérvese, sin embargo, que se trata de una medida formal puesto que sólo se trata de informar a la Agencia de Protección de Datos, que deberá asegurarse de la procedencia o no de la decisión, pero que en ningún caso tiene otras consecuencias jurídicas, ya que no se establece una vinculación del responsable del fichero respecto de la decisión de la Agencia.

Asimismo, se excluye el ejercicio del derecho de información por el afectado cuando ello «impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas» (art. 24.1 LOPD). Claro que a este respecto, y siguiendo las afirmaciones del Defensor del Pueblo en su recurso de inconstitucionalidad contra los arts. 24. 1 y 2 de la LOPD si la restricción del derecho a la información encuentra cobertura legal en las previsiones del Convenio 108 (art. 9) y de la Directiva 95/46/CE (art. 13) cuando su ejercicio afecte a la

defensa nacional, a la seguridad pública o a la persecución de infracciones penales; no sucede lo mismo en el caso de que se exceptúe su ejercicio cuando «impida o dificulte gravemente el cumplimento de las funciones de control y verificación de las administraciones públicas»[59] ni cuando «afecte a la persecución de infracciones administrativas»[60], lo que significa que el legislador se ha extralimitado en su deber de respeto al contenido esencial del derecho a la protección de datos, al imponer más límites a su ejercicio de los que resultan necesarios y razonables para la tutela de otros bienes o valores constitucionales.

Ahora bien, se exceptúa también el ejercicio de los derechos de acceso, rectificación o cancelación «si ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de protección de datos o, en su caso, del órgano equivalente de las comunidades autónomas» (art. 24.2 LOPD). Y en este punto ha sido especialmente crítico

---

[59] A este respecto ha insistido el TC en su STC 292/2000 en que «el empleo por la LOPD en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa… Lo que a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y suma en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia».

[60] En relación con este supuesto, ha declarado el TC que «la posibilidad de que con arreglo al art. 24.1 LOPD, la Administración pueda sustraer al interesado información relativa al fichero y sus datos, según dispone el art. 5.1 y 2 LOPD, invocando los perjuicios que semejante información pueda acarrear a la persecución de una infracción administrativa, supone una grave restricción a los derechos a la intimidad y a la protección de datos carente de todo fundamento constitucional. Y cabe observar que se trata, además, de una práctica que puede causar grave indefensión en el interesado, que puede verse impedido de articular adecuadamente su defensa frente a un posible expediente sancionador por la comisión de infracciones administrativas al negarle la propia Administración acceso a los datos que sobre su persona pueda poseer y puedan ser empleados en su contra sin posibilidad de defensa alguna al no poder rebatirlos por resultarle ignotos al afectado».

el TC con el abusivo empleo de conceptos jurídicos indeterminados para excepcionar el ejercicio de los derechos de protección de datos, por ello censura «el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor que la expresión utilizada en el art. 24.1 LOPD. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE» (STC 292/2000, de 30 de noviembre).

Para concluir, nada tan oportuno como hacer propias las acertadas reflexiones del TC en las que advierte que la legitimidad constitucional de la restricción del derecho a la protección de datos personales no puede fundarse exclusivamente en la actividad de la Administración. Ni tan siquiera es suficiente que la Ley apodere a la Administración para que establezca los límites que en cada caso deban concurrir, es el legislador, quien debe determinar cuándo concurre algún bien o derecho constitucionalmente protegido, que justifique la restricción del derecho a la protección de datos, porque en otro caso, se traslada a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales a tenor del principio de reserva de Ley, cual es establecer el límite y la regulación de estos derechos.

4. El movimiento internacional de datos personales

De forma temprana se adquiere conciencia de los importantes problemas que podía plantear el flujo internacional de datos personales tanto en el sector público, como en el ámbito privado. Nacen entonces las Directrices de la OCDE sobre Protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras, que intentan prevenir a los Estados sobre la necesidad de evitar prácticas o directrices políticas que en nombre de la protección de la intimidad y de las libertades individuales, excedan las exigencias de dicha tutela y dificulten o impidan la transmisión de datos personales a través de las fronteras[61].

En la LOPD, el principio general sobre transmisiones de datos personales a terceros países establece que no podrán realizarse transferencias

[61] Cfr. Recomendación de la OCDE de 23 de septiembre de 1980, sobre las directrices de protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras.

de datos personales que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no garantizan un nivel de protección equiparable al de la LOPD, salvo que se observe lo dispuesto en la Ley y además se obtenga autorización previa del Director de la Agencia de protección de datos, que sólo podrá concederse si se prestan las garantías adecuadas. Sorprende que el legislador español en contra de las previsiones comunitarias insista en establecer un principio general de prohibición de las transferencias internacionales de datos.

Por otro lado, se aprobó el 1 de diciembre la Instrucción 1/2000 relativa a las normas por las que se rigen los movimientos internacionales de datos[62], que en su norma quinta hace referencia a las transferencias internacionales de datos a un Estado no comunitario, respecto del que no se haya declarado la existencia de un nivel adecuado de protección, y el transmitente se funde en las excepciones del art. 34 LOPD, entonces la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación. Cuando la transferencia no se funde en alguno de los supuestos del art. 34 o cuando esta circunstancia no haya quedado debidamente acreditada, será necesario autorización del Director de la Agencia de Protección de Datos, autorización que procederá cuando el responsable del fichero aporte un contrato escrito celebrado entre transmitente y destinatario, en el que consten las garantías de respeto a la intimidad de los afectados y a sus derechos y libertades fundamentales. Remitido el contrato, la Agencia podrá solicitar que se introduzcan las modificaciones oportunas para garantizar el cumplimiento de las exigencias legales en un plazo de diez días, transcurrido el cual, y sin que se haya cumplido con esta exigencia, se denegará la autorización. Una vez que se ha autorizado la transferencia, ésta deberá inscribirse en el Registro General de Protección de Datos y se procederá a su comunicación a la Comisión de las Comunidades Europeas. Ello no obstante, el Director de la Agencia excepcionalmente y por los supuestos tasados legalmente podrá denegar o suspender temporalmente, la transferencia previa audiencia del transmitente[63].

---

[62] Cfr. BOE núm. 301, de 16 de diciembre de 2000.

[63] Se hace referencia a supuestos tales como: el incumplimiento de las garantías contractuales, la existencia de indicios racionales sobre el incumplimiento de las garantías contractuales o sobre la inefectividad de los mecanismos de aplicación del contrato, o cuando la transferencia ya iniciada pueda crear riesgo de daño efectivo para los afectados, y finalmente, cuando la situación de protección de los derechos fundamentales y libertades públicas en el país destinatario o en su legislación impidan garantizar el cumplimiento del contrato y el ejercicio de los derechos del afectado.

Nada prevé la LOPD sobre los flujos pasivos de datos personales, aquellos que tienen como origen de la transmisión un país tercero, siendo España el país de destino. Igualmente ha de lamentarse que no se contemplen normas sobre el flujo de datos personales registrados en fuentes accesibles al público, o sobre las transmisiones internacionales como consecuencia de relaciones contractuales y comerciales entre empresas vinculadas jurídicamente, o el flujo que se mantiene con fines comerciales. Sin embargo, la Instrucción 1/2000 regula las transferencias que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, cuya ejecución se regulará en un contrato, en el que constará la responsabilidad directa del transmitente como consecuencia de cualquier incumplimiento legal (norma sexta). Se garantizará que cumplida la prestación contractual, los datos personales serán destruidos o devueltos al transmitente, asegurando que no podrán ser cedidos a terceros. Si el destinatario está en un Estado no comunitario que no asegura un nivel de protección adecuado, se seguirán las cautelas previstas para estas transferencias en la Instrucción 1/2000.

Excepcionalmente, podrán realizarse transferencias internacionales de datos aunque no se cumplan las previsiones del art. 33 cuando, además de los supuestos contemplados en el art. 26 de la Directiva 95/46/CE, la transferencia internacional de datos:

a) resulte de la aplicación de tratados o convenios en los que es parte España, o cuando se haga para prestar o solicitar auxilio judicial internacional
b) tenga como destino un Estado miembro de la Unión Europea, o un Estado que la Comisión de las Comunidades Europeas ha declarado que garantiza un nivel de protección adecuado.

5. *La autoridad de control. La Agencia de Protección de datos*

Ya el Convenio 108 del Consejo de Europa impulsa a los Estados a designar autoridades de control para la protección de datos, si bien nada establece respecto a sus funciones ni a los criterios que debían inspirar su regulación (art. 13.2). Después será la Directiva 95/46/CE la que establezca la necesidad de la creación de la autoridad de control, al tiempo que prevé los criterios precisos para su regulación (Considerandos 62 y 63 Directiva 95/46/CE).

En el ámbito autonómico, la primera Agencia de Protección de Datos se crea en la Comunidad de Madrid, en virtud de la Ley 13/95, de

21 de abril. En la actualidad, se ha aprobado la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, y también la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos[64].

4.1. Naturaleza y régimen jurídico de la Agencia de protección de datos

No puede menospreciarse el protagonismo que la Agencia de Protección de Datos alcanzará en el orden constitucional como garante de los derechos fundamentales y libertades individuales de las personas frente al tratamiento de datos personales. Por ello, la Agencia de Protección de Datos tiene la consideración legal de un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con absoluta independencia de las Administraciones públicas en el ejercicio de sus funciones, y se regirá por un Estatuto propio[65], aprobado por el Gobierno. Por tanto, la Agencia se constituye como administración independiente[66], y no se encuentra sometida jerárquicamente a la estructura y organización del Estado, ya que sólo será posible el control de legalidad por los órganos judiciales y la destitución de su Director únicamente tendrá lugar por los supuestos legalmente establecidos; sin embargo, han sido muchas las reservas que la doctrina ha mantenido respecto a la consideración de la Agencia como administración independiente[67].

En el ejercicio de sus funciones públicas, y salvo lo dispuesto en la LOPD, y en sus normas de desarrollo, la Agencia actuará de conformidad con la Ley 30/92 de 26 de noviembre, si bien en sus adquisiciones patrimoniales y contratación se someterá al derecho privado.

Las funciones de la Agencia de Protección de Datos pueden clasificarse atendiendo a los diversos fines a que responden. Ejerce la Agencia *funciones de control*, de los tratamientos de datos personales, tales como velar por el cumplimiento de las normas sobre protección de datos

---

[64] Cfr. Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, BOE núm. 245, de 12 de octubre de 2001 y Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, BOE núm. 115, de 14 de mayo de 2002.

[65] Cfr. Real Decreto 428/1993, de 26 de marzo, de aprobación del Estatuto de la Agencia de Protección de Datos, BOE núm. 106, de 4 de mayo de 1993 (en adelante EAPD).

[66] López Ramón, Fernando, «La Agencia de Protección de Datos como Administración independiente», *Jornadas sobre el Derecho español de la protección de datos,* Madrid, Agencia de Protección de Datos, 1996.

[67] Herrán Ortiz, Ana I., *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, *op. cit.,* p. 327.

o requerir a los responsables y los encargados de los tratamientos la adopción de medidas necesarias para la adecuación de los tratamientos a la Ley y controlar los datos personales introducidos en la Parte nacional española de la base de datos del Sistema de Información de Schengen.

Ejerce también la Agencia *funciones de inspección*, por lo cual podrán inspeccionar todos los ficheros sujetos la Ley, recabando cuantas informaciones precise para el cumplimiento de su cometido. La actuación inspectora de la Agencia se concreta en la solicitud de la «exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados» (art. 40.2 LOPD). Para cumplir esta función, compete a la Agencia efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros, de titularidad privada o pública, en los locales mismos donde se hallen los ficheros y equipos informáticos correspondientes. En definitiva el principal objetivo de la actuación inspectora no es otro que supervisar y garantizar la seguridad de los sistemas de tratamiento de datos, no en vano entre las funciones que tiene asignadas se encuentran el examen de los soportes de información, de los equipos físicos, y de transmisión y acceso a los datos (art. 28.1 EAPD).

Las funciones de control y vigilancia precisan para ser efectivas del ejercicio de la *función sancionadora*, por la cual podrá ordenar la cesación de los tratamientos y la cancelación de los ficheros que no se ajusten a la Ley. Pero además desarrolla la Agencia *funciones normativas*, y así podrá aprobar instrucciones para adecuar los distintos tratamientos de datos a la legalidad, y dictar recomendaciones de aplicación de las disposiciones normativas, al tiempo que deberá informar sobre proyectos de disposiciones generales que desarrollen la Ley.

Tiene atribuidas la Agencia *funciones de tutela* de los derechos de las personas, por lo que podrá atender las peticiones y reclamaciones formuladas por los afectados, y podrá proporcionar información sobre los derechos en materia de protección de datos. Para el cumplimento de esta obligación la Agencia tiene reconocida una *función de publicidad* de los tratamientos y de su propia actividad; por la primera le corresponde velar por la publicidad de la existencia de los ficheros y por la segunda, debe la Agencia elaborar una Memoria anual sobre aplicación de la Ley y sobre sus propias actividades y funcionamiento.

Y por último, la Agencia deberá desarrollar *funciones de cooperación institucional*, por cuanto que tiene encomendada la cooperación con organismos internacionales y con los órganos de las Comunidades

Europeas en materia de protección de datos (art. 9 EAPD). Pero también cooperará y colaborará con los órganos correspondientes de las Comunidades Autónomas (art. 41.3 LOPD)[68].

4.2. La estructura organizativa de la Agencia. La figura del Director

Ha lamentado la doctrina que la estructura de la Agencia no se haya previsto desde una organización colegiada, que reduzca el protagonismo del Director, y refuerce el del Consejo Consultivo como órgano de decisión, lo que además evitaría la acumulación de poder e influencia en el Director, y equilibraría la adopción de decisiones en el Consejo Consultivo[69].

Dice el art. 36.1 LOPD que el Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Abundando en lo expresado, el EAPD en su art. 2.3 establece que la Agencia ejercerá sus funciones a través del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia. Con ello, se evidencia el especial protagonismo de la figura del Director que se configura como eje central de la Agencia de Protección de Datos. El Director será nombrado de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Corresponde al Gobierno el nombramiento del Director, a propuesta del Ministro de Justicia, de entre los miembros del Consejo Consultivo (art. 14 del Estatuto de la Agencia).

El Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones, claro que no se trata de una propuesta vinculante, ni que condicione la actuación del Director, sino más bien de una exigencia formal que deberá observar el Director. Ha sido también cuestión muy debatida la regulación del cese del Director, que tendrá lugar «a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso» (art. 36.3 LOPD). Así, la intervención del Consejo Consultivo tanto en el nombramiento como en el cese anticipado del

---

[68] Troncoso Reigada, Antonio, «La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos», *XVII Encuentros sobre Informática y Derecho*, Universidad Pontificia Comillas, Madrid, 2003, pp. 23-45.

[69] Roca Junyent, Miguel y Torralba Mendiola, Elisa, «La Ley de protección de Datos», *La Ley,* núm. 2, 2000, p. 7.

Director resulta meramente testimonial, porque únicamente serán oídos, ya que corresponde adoptar la decisión al Gobierno.

Respecto a las funciones que tiene atribuidas el Director, hay que diferenciar por un lado, las funciones de dirección, y por otro, las funciones de gestión. Las primeras se refieren a los actos necesarios para llevar a cabo la dirección de la Agencia de Protección, así, la facultad de dictar resoluciones e instrucciones para la tutela de las personas en lo que respecta al tratamiento de sus datos; las segundas, son las propias y necesarias para el funcionamiento de la Agencia como organismo o institución, y se refieren al control económico-financiero, la aprobación de gastos, la adjudicación de contratos, la propuesta de puestos de trabajo, son funciones que a excepción de la aprobación de la Memoria Anual y el control del gasto y convocatoria del Consejo Consultivo podrán delegarse en el Secretario General.

El Director estará asesorado por el Consejo Consultivo que no asume tareas directivas, ni adopta decisiones en cuanto al funcionamiento de la Agencia (art. 38 LOPD). Integran el Consejo Consultivo representantes de ambas Cámaras Legislativas, del Gobierno Central, de la Administración Local y Autonómica, del ámbito de la cultura y las instituciones, y de algunos de los sectores implicados en la protección de datos (art. 38 LOPD).

Por su parte, y para dar cumplimiento al principio de publicidad de los tratamientos, el Registro General de Protección de Datos, como órgano de la Agencia velará por la publicidad de los ficheros de datos personales, para hacer posible el ejercicio de los derechos reconocidos a los interesados en la LOPD. Además también se inscribirán en el Registro las autorizaciones de transferencias de datos a otros países y los códigos-tipo.

IV. **A modo de conclusión**

La interpretación por la jurisprudencia constitucional del art. 18.4 CE ha permitido establecer una definición jurídica precisa del derecho a la protección de datos personales. Así, al tiempo que se ha reconocido la aparición de una nueva garantía constitucional que ofrece cumplida respuesta a las nuevas formas de amenaza que la informática trae consigo para los derechos de las personas, se han establecido los criterios que configuran este nuevo derecho fundamental a la protección de datos y que lo diferencian de otros derechos tradicionalmente reconocidos, como el derecho a la intimidad personal y familiar o el derecho al honor. En este sentido, siguiendo las afirmaciones del Tribunal Constitucional, el derecho a la protección de datos extiende su garantía no sólo a la intimidad, sino a otros bienes y derechos de la personalidad; así, también dispone el derecho a la protección de datos de un contenido esencial específico, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera privada de la persona. Por tanto, si la función del tradicional derecho a la intimidad es proteger a la persona frente a cualquier injerencia en el ámbito de su intimidad personal y familiar, el derecho fundamental a la protección de datos pretende atribuir y garantizar un poder de control y disposición sobre los datos personales, con el propósito de impedir un tratamiento ilícito y lesivo para la dignidad y los derechos y libertades del afectado.

Por otra parte, la aprobación de la Directiva 95/46/CE sobe protección de datos personales, además de establecer un nuevo marco comunitario para la protección de las personas frente al tratamiento de sus datos, significó para el legislador español una nueva oportunidad para abordar la regulación de la protección de datos personales; sin embargo, pronto se frustraron las expectativas que la trasposición de la Directiva 95/46/CE había generado, y fueron muchas las cuestiones que en la nueva regulación no han encontrado una respuesta satisfactoria; así, entre otros pueden citarse la regulación de las fuentes de acceso público, el tratamiento de las categorías especiales de datos, la excepcional regulación de los ficheros públicos o el régimen sancionador.

De la nueva Ley Orgánica 15/99 destacan especialmente dos aspectos: por un lado, la extensión de su ámbito de aplicación a todo tipo de tratamientos, automatizados o no, de datos personales; y, por otra parte, la incorporación de nuevos derechos del interesado, como el de oposición al tratamiento, o el de indemnización por los daños que ocasione el tratamiento. Ello no obstante, sin embargo, han sido numerosas y significativas las carencias de la Ley, que ha insistido en errores

que ya habían sido objeto de crítica en la anterior regulación, y que merecieron en algunos casos la interposición de recursos de inconstitucionalidad. Así, el excepcional régimen regulador de los ficheros de datos en el sector público que permitía sin el consentimiento del interesado la cesión de datos entre Administraciones públicas cuando la disposición de creación del fichero u otra de igual rango lo autorice constituyó uno de los aspectos más controvertidos de la nueva Ley. Por ello, ha de felicitarse la decisión del TC que en STC 292/2000 ha declarado dicha norma nula por inconstitucional, y ha censurado que LOPD no haya fijado expresamente, tal y como la Constitución exige, los límites al derecho a consentir la cesión de datos entre administraciones, para fines diferentes a los que motivaron su recogida, vulnerando así el principio de legalidad.

De igual forma fueron declaradas nulas e inconstitucionales las excepciones al ejercicio de los derechos del afectado frente a los ficheros públicos cuando así se justifique para «la prevención de un peligro real», «para el cumplimento de las funciones de control y verificación de las Administraciones Públicas», «por razones de intereses públicos o intereses de terceros más dignos de protección». Denuncia el TC la indeterminación de los conceptos empleados por el legislador, que conceden excesiva discrecionalidad a la actuación administrativa, lo que significa una remisión en blanco del poder legislativo, y causa indefensión al interesado, que no podrá acceder, ni rectificar o cancelar la información en poder de la Administración pública.

En otro orden de consideraciones, la sociedad de la información desarrolla constantemente nuevos medios de comunicación lo que ofrece al legislador importantes retos normativos, ante la necesidad de conciliar estos avances tecnológicos con los derechos y libertades fundamentales de la persona; por ello, la protección de datos personales en el ámbito de las telecomunicaciones presenta especiales caracteres que aconsejan adoptar una regulación específica. Así se ha entendido en el ámbito comunitario, que ha adoptado sucesivas Directivas para garantizar la protección de datos personales en las comunicaciones electrónicas, la última de ellas la Directiva 58/2002/CE, y afortunadamente, así lo ha considerado también el legislador español que en la LOPD no entra a regular la protección de datos personales en la prestación de servicios de telecomunicación, y remite a la normativa específica que al respecto se apruebe.

Para finalizar, ha de lamentarse la falta de conciencia de los ciudadanos sobre la necesidad de proteger la información que les concierne, y es de esperar que la Agencia de Protección de Datos como institución garante de los derechos de las personas frente al trata-

miento de sus datos realice un esfuerzo de aproximación a los ciudadanos y les ayude a comprender la verdadera importancia del derecho a la protección de datos personales; no hay que olvidar por otra parte, que desde las propias Comunidades Autónomas se ha comenzado a aprobar legislaciones en materia de protección de datos, lo que se ha traducido en la aparición de las nuevas autoridades de control autonómicas, que en el ámbito de sus competencias deberán desarrollar una actividad coordinada con la Agencia estatal de Protección de Datos.

Cuadernos Deusto de Derechos Humanos, núm. 26

No puede cuestionarse que en la actualidad se han transformado las formas de relación, y ello es debido en parte al imparable avance tecnológico, y fundamentalmente a la irrupción de la informática y de las nuevas formas de comunicación. Pero al mismo tiempo estos fenómenos han significado una amenaza para la garantía de los derechos individuales; por ello, resultará necesario conciliar el desarrollo tecnológico con el obligado respeto a los derechos de la persona. Y es a esta última cuestión a la que se pretenderá dar respuesta en este estudio, no en vano la protección de los derechos y libertades fundamentales no ha de ceder ni quebrar ante la utilización de las tecnologías de la información y la comunicación.

Ana Isabel Herrán Ortiz. Master en Asesoría Jurídica de Empresas por la Universidad de Deusto. Doctora en Derecho por la Universidad de Deusto. Experta en Derecho de las Tecnologías de la Información y la Comunicación. Profesora Titular de Derecho civil de la Universidad de Deusto. Autora de importantes publicaciones sobre el derecho de protección de datos personales, entre otros ha publicado los libros: *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales* y *La violación de la intimidad en la protección de datos personales*. Asimismo, ha publicado recientemente artículos sobre *La Directiva europea 95/46/CE de protección de datos personales* y *La protección de datos en la jurisprudencia constitucional*, entre otros.

EUSKO JAURLARITZA
GOBIERNO VASCO

JUSTIZIA, LAN ETA GIZARTE SEGURANTZA SAILA

DEPARTAMENTO DE JUSTICIA, EMPLEO Y SEGURIDAD SOCIAL

Universidad de Deusto