



Revista de Fomento Social, 52 (1997), 313-344

## Régimen jurídico del tratamiento automatizado de los datos de carácter personal

---

*La revolución tecnológica y mediática ha ampliado en forma inusitada las formas de inmisión o intromisión en la esfera más íntima de la persona. En forma paralela la información, controlada y manipulada por escasas manos, deviene una fuente de poder extraordinaria y refractaria a los controles tradicionales. En este nuevo contexto la labor judicial y doctrinal construye afanosamente nuevos derechos fundamentales, como el derecho de libertad informática, que sirven de trinchera de contención y represión a los ataques más graves e injustificados a la privacidad de los ciudadanos. Con el Convenio núm. 108 del Consejo de Europa de 1981 como paradigma, el legislador español promulgó en 1992 una normativa sobre tratamiento automatizado de datos de carácter personal que, junto al avance que ya supone una regulación ad hoc en la materia, introduce importantes normas que merecen una severa crítica. Actitud que hay que mantener ante la reciente Directiva de 1995 sobre tratamiento automatizado de datos personales y libre circulación de estos datos.*

---

Manuel PANIAGUA ZURERA (\*)

---

(\*) Prof. Titular Derecho Mercantil. Facultad CC.EE. y Empresariales (ETEA).

## I. Planteamiento

En las sociedades de la posmodernidad, de la revolución tecnológica y mediática, y del consumo, la información se ha convertido en una fuente de poder. En estos contextos la información personal deviene un bien inmaterial, susceptible de lesiones diversas y, al mismo tiempo, un bien objeto de tráfico patrimonial. Si adicionamos la posibilidad —antes inexistente— del tratamiento automatizado de datos de carácter personal, nos encontramos con que esta información personal puede viajar, puede ser negociada, puede ser interrelacionada conformando el perfil económico, sociológico, ideológico, laboral, etc. de la persona. Esta auténtica disección personal, gestada con datos procedentes de fuentes diversas, tiene una trascendencia enorme, pues es —o puede ser— la base para obtener o no un empleo, un crédito, la admisión en determinadas entidades, etc. En efecto, los riesgos potenciales de intromisión en lo más íntimo de la persona y de discriminación por datos estrictamente personales, cobran virtualidad en las sociedades avanzadas del primer mundo donde, a finales del segundo milenio, la ausencia de conocimientos informáticos constituye *de facto* una nueva modalidad de analfabetismo.

Ante el tímido, en un primer momento, peligro de intromisión informática aparecen las primeras Leyes a inicios de los setenta (Estado alemán de Hesse 1970, Suecia 1973, Estados Unidos 1974, República Federal Alemana 1977, y Francia 1978), centradas en la protección del derecho a la intimidad. Las primeras Leyes tienen en mente intromisiones procedentes del poder público o, como mucho, procedentes de grandes empresas, que eran los únicos que disponían de los costosos y aparatosos medios informáticos en que se concretaron la primera generación de ordenadores, y a tal efecto contemplan un conjunto de medidas sancionadoras *a posteriori*.

Había pasado una década cuando ya se intuía la popularización de los ordenadores, auspiciada por los avances vertiginosos en microinformática. La información podía ser tratada y transferida por y a más operadores, de ahí la necesidad de una tutela preventiva frente a posibles violaciones de la intimidad personal. Por otro lado, como en el ámbito del Derecho de propiedad industrial y del Derecho de propiedad intelectual, se advierte que una tutela del tratamiento de datos personales en una esfera nacional es totalmente ineficaz, pues basta la transferencia de esos datos a otro Estado para que puedan ser utilizados en

formas prohibidas en el país de origen. No es casualidad que el siguiente paso en este sentido lo encontramos en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos de carácter personal de 28 de enero de 1981 que, como advierte su Preámbulo, intenta «ampliar el ámbito de las garantías de los derechos y libertades fundamentales de toda persona, en especial el Derecho a la intimidad».

La revolución informática ha continuado avanzando a pasos acelerados, tanto en forma cuantitativa (mejores y más potentes ordenadores a precios más accesibles), como cualitativa (avances en programas *—software—*, en interconexiones informáticas y telecomunicaciones). En esta línea el principal protagonista es *internet*. Las investigaciones militares norteamericanas dirigidas a la creación de una red de conexión informática que no pudiese ser neutralizada ni interrumpida por catástrofes naturales o por conflictos bélicos comienzan en la década de los sesenta. Sus resultados van a ser perfeccionados en Europa en nuestra década, dando origen a un sistema de transmisión de datos en sentido amplio (textos, imágenes y sonidos) que es denominado con las abreviaturas «WWW» (*word wide web*), cuya traducción aproximada es la *telaraña* mundial o la gran red mundial. Esta red de redes tiene como instrumento y servicio básico el hoy familiar *internet*, en el que junto a esta interconexión informática, se ofrecen los servicios más variados (correo electrónico, transferencia de archivos, comunicaciones en tiempo real, acceso a bases de datos, comercio electrónico, etc.), algunos de ellos de dudosa legalidad (v.gr.: acceso a archivos protegidos, publicación de ciertas informaciones, ciertas modalidades de ventas, etc.), cuando no de flagrante ilegalidad (v.gr.: pornografía infantil, venta de órganos, alquiler de úteros, estafas informáticas, violaciones a la propiedad intelectual e industrial, etc.). Ante estos avances *—con las cautelas que lo desconocido impone—* la protección de los datos personales frente a su tratamiento informático tiene un reto en buena medida pendiente: incardinar esta protección frente al tratamiento de datos personales entre los derechos fundamentales de la ciudadanía. Los primeros pasos ya se están dando, precisamente va a ser el avance doctrinal, propiciado por la ejemplar jurisprudencia de algunos Tribunales Constitucionales *—especialmente el de la entonces República Federal Alemana en su Sentencia de 15 de diciembre de 1983 con la teorización sobre el «derecho a la autodeterminación informativa»—* el que va destilando un nuevo derecho humano de la tercera generación: el derecho a la libertad

informática (Herederó Higueras, 1992, 2-3; López-Ibor Mayor, 1993, 2-3; Velázquez Bautista, 1993, 66-69; y, especialmente, Pérez Luño, 1996, 43-46). No obstante, la cuestión no es pacífica en la doctrina, pues un importante sector defiende que estamos sólo ante una ampliación de la tutela del derecho a la intimidad o de los derechos fundamentales en general (López Díaz, 1996, 247; y, como ejemplo en la doctrina civil, Díez-Picazo y Gullón, 1995, 248-250).

La legislación española se queda, al menos en su letra, a mitad de camino entre la segunda y tercera etapas descritas. La Ley 5/1992, de 29 de octubre, sobre regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) (BOE núm. 262, de 31 de octubre) va más allá de la idea de intimidad, e introduce la noción de *privacidad* como concepto más amplio que abarcaría más facetas de la personalidad de los ciudadanos (v. *infra*).

## II. La libertad informática en la Constitución española de 1978

Con un enfoque menos amplio, y más anclado en el concepto de intimidad, el artículo 18.4 Constitución (CE) establece: «*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*». El precepto carece de antecedentes en nuestra historia constitucional. Tenemos que acudir a nuestro vecino para congratularnos con la previsión contenida en el artículo 35 de la Constitución portuguesa de 1976:

«1. *Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanografiados acerca de ellos y la finalidad a la que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.*

2. *No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.*

3. *Se prohíbe atribuir un número nacional único a los ciudadanos*».

El contenido del actual art. 18.4 CE ya aparecía en el Anteproyecto constitucional, si bien referido a la limitación del uso de la informática respecto

a los derechos al honor y a la intimidad personal y familiar. El Dictamen de la Comisión del Congreso le dio la redacción final, con la acertada referencia al ejercicio de los restantes derechos de los ciudadanos.

Dada su ubicación constitucional (Sección 1ª, Capítulo II del Título Primero) el derecho a la libertad informática vincula a todos los poderes públicos —y a los sujetos de Derecho privado ex art. 9.1 CE—, y su regulación exige una Ley —que habrá de ser orgánica ex art. 81.1 CE— que, en todo caso, debe «*respetar su contenido esencial*». Por otro lado, del control constitucional de este desarrollo legal se encarga el Tribunal Constitucional ex art. 161.1 letra a) CE (de hecho están pendientes cuatro recursos de inconstitucionalidad contra determinados artículos de la LORTAD). Finalmente, para la tutela de este derecho los ciudadanos pueden acudir ante la jurisdicción ordinaria a través de un procedimiento «*basado en los principios de preferencia y sumariedad*» (véanse la Ley 62/1978, de 26 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona; la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen; y la Ley Orgánica 2/1984, de 26 de marzo, sobre el derecho de rectificación) y, tras agotar los recursos ordinarios, acudir en amparo ante el Tribunal Constitucional (art. 53.1 y 2 CE).

El artículo 18.4 CE ha merecido escasa atención por parte de la doctrina (Sempere Rodríguez, 1984, 436–439; y, con mayor extensión, Serrano Alberca, 1985, 377–381), absorbido como está en un precepto donde se recogen los derechos al honor, a la intimidad personal y a la propia imagen. No obstante, no faltan análisis panorámicos de la incidencia de la informática en el ejercicio de los distintos derechos constitucionales (Velázquez Bautista, 1993, 35–73).

Poco después de promulgada nuestra Constitución se intensifica la actividad del Consejo de Europa en la tutela de la intimidad y privacidad frente a las posibles invasiones informáticas, cuyos primeros pasos arrancan en septiembre de 1973. Este interés culmina en el citado Convenio 108, de 28 de enero de 1981, ratificado por España en 1984 y publicado en el BOE núm. 274, de 15 de noviembre de 1985. El Convenio 108 no es una norma directamente aplicable, pues los Estados han de adoptar «*en su Derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos*» (art. 4). No obstante, el contenido de este Convenio ha estado presente en la mente del legislador español cuando se proyecta la LORTAD, y no debemos olvidar

que, por aplicación del art. 10.2 CE, la normativa sobre derechos y libertades fundamentales recogidos en la Constitución «*se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España*». En el Convenio 108 se acoge una tutela preventiva del derecho a la libertad informática que es la que, mejor o peor, recibe más de una década después la Ley Orgánica 5/1992, de 29 de octubre, sobre regulación del tratamiento automatizado de los datos de carácter personal.

Como en el desarrollo de otros preceptos constitucionales, la concreción normativa del mandato contenido en el art. 18.4 CE no ha sido el propósito legislativo de dar sustancia al derecho a la libertad informática. Por el contrario, el detonante último de la LORTAD —a pesar de la existencia de declaraciones sobre el necesario desarrollo del art. 18.4 CE desde mediados de 1983— fue la necesidad de cumplir el Acuerdo de Schengen, de carácter eminentemente policial (Fernández Calvo, 1993, 4). Conviene advertir —aunque no entramos en su comentario— que sobre algunos preceptos de la LORTAD se ciernen serias dudas de constitucionalidad, de hecho han presentado recursos de inconstitucionalidad el Grupo Popular, el Defensor del Pueblo, y el Gobierno y Parlamento Catalán (Quílez Agreda y Cebrián del Moral, 1993, 6–7). En concreto, junto a la cuestión competencial planteada desde Cataluña, se cuestionan dos temas delicados: 1º la cesión de datos entre Administraciones Públicas (art. 19 LORTAD), y 2º las numerosas excepciones a los derechos de los ciudadanos que la LORTAD posibilita (v. *infra*).

### III. La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal

Hasta la aparición de la LORTAD, la Disposición Transitoria 1ª de la citada Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y a la propia imagen estableció que, en tanto no se desarrollase el art. 18 CE, las intromisiones en estos derechos a través de procedimientos informáticos se regularían por lo previsto en esta Ley (Díez-Picazo y Gullón, 1995, 249). La Ley 5/1992 supone el desarrollo del mandato constitucional del art. 18.4 CE. Su extensa Exposición de motivos establece como finalidad de la LORTAD el hacer frente a los riesgos que para los derechos de la personalidad puede suponer

la recogida y el tratamiento de datos por procedimientos informáticos. La propia Exposición advierte de las amenazas a la *privacidad*, y no a la simple intimidad, concepto el primero más amplio, en cuando a través de estos datos personales —datos que pueden estar muy separados en el espacio y en el tiempo, lo que en otras épocas era suficiente para su protección— y su interconexión informática se puede establecer un determinado perfil de la persona, y este perfil puede ser valorado positiva o negativamente y tener trascendencia en actividades diversas (obtención de un empleo, concesión de un crédito, admisión en determinados colectivos, por ejemplo). En los términos de la propia Exposición de motivos:

*«El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado».*

La LORTAD supone un desarrollo tardío del texto constitucional, que ha merecido serias objeciones críticas (López-Ibor Mayor, 1993, 1–4; Pérez Luño, 1996, 47–67). Por su trascendencia destacan estas dos:

- 1º) Las continuas excepciones que la propia Ley introduce a sus normas protectoras y las remisiones a normas reglamentarias (v. a título de ejemplo los artículos 2.2 y 3, 4.5, 5.3, 6.2, 7.3 y 5, 9.3, 11.2, etc.). Este proceder sin duda afecta al contenido esencial del derecho a la libertad informática ex art. 18.4 CE, así como al rango normativo con el que debe regularse. Las aludidas excepciones —que seguidamente comentamos— son muy llamativas cuando las comparamos con la generosidad del

Convenio 108 del Consejo de Europa que sólo excluye de su ámbito de aplicación aquellos ficheros sometidos a una legislación específica sobre protección de datos. No obstante, como veremos, la reciente Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 introduce importantes posibilidades para excepcionar determinados ficheros (Martín-Casallo López, 1996, 4).

- 2º) La estructuración de la Agencia de Protección de Datos (APD), que más que un organismo independiente —como afirma el art. 34.2 de la Ley—, permite una fuerte control gubernativo, pues su Director es nombrado por el Gobierno mediante Real Decreto (art. 35.1). Las dudas sobre la independencia e imparcialidad de este organismo público pueden frenar la eficacia de la normativa que comentamos, y el surgimiento de una conciencia colectiva que actúe de barrera frente a los abusos en el tratamiento informático de datos personales. De ahí que tenga gran importancia la ejemplaridad de las instrucciones y decisiones de la APD.

La LORTAD ha previsto importantes remisiones a ulteriores desarrollos reglamentarios que, en los años sucesivos, se han ido produciendo. Las normas en cuestión son: 1º) el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE núm. 106, de 4 de mayo), modificado por Real Decreto 156/1996, de 2 de febrero (BOE núm. 37, de 12 de febrero) para designar a esta Agencia como representante español en el Grupo de Protección de Personas previsto en la Directiva 95/46/CE, de 24 de octubre, al que posteriormente nos referimos; y, 2º) el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la EORTAD (BOE núm. 147, de 21 de junio).

Sin entrar por ahora en la regulación de la Agencia de Protección de Datos, de la que nos ocupamos más adelante, el contenido de la LORTAD puede ser sistematizado en estos términos: 1º) objeto y ámbito de aplicación; 2º) régimen general de la creación de los ficheros de datos; 3º) derechos de los afectados; 4º) normas especiales para los ficheros de titularidad pública y los de titularidad privada; y 5º) infracciones y sanciones administrativas. Seguidamente abordamos cada una de estas partes.

### 1. Objeto y ámbito de aplicación

El objetivo que persigue la LORTAD es limitar el tratamiento automatizado de datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las «*personas físicas*» (por ahora quedan fuera las personas jurídicas, aunque en un futuro tendrá que revisarse esta limitación) y el pleno ejercicio de sus derechos (art. 1). Como regla, la Ley se aplica a todos los datos de carácter personal que figuren en ficheros automatizados, sean de titularidad pública o privada, «*y a toda modalidad de su uso posterior, incluso no automatizado*» (art. 2.1). El art. 1.3 R.D. 1332/1994 establece que, a sus efectos, la expresión «*datos de carácter personal*» tiene este sentido: «*toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable*». Como podemos advertir raro será el organismo público, el empresario individual o colectivo, las asociaciones, las fundaciones, etc. que no tengan uno de estos ficheros con datos personales.

Ahora bien, la propia Ley establece numerosas e importantes excepciones a su ámbito de aplicación: ficheros públicos para su publicidad general; ficheros privados para fines personales; ficheros que recojan datos publicados en boletines o diarios oficiales; ficheros de partidos políticos, sindicatos y confesiones religiosas sobre sus miembros o ex miembros (art. 2.2). El art. 1.4 R.D. 1332/1994 concreta el significado jurídico de la expresión «*datos accesibles al público*» a los efectos de esta normativa de desarrollo. Por su transcendencia para la aplicación de la normativa que comentamos lo transcribimos, pese a su extensión. El citado precepto dispone: «*Datos accesibles al público: los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombre, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo*».

Asimismo, la LORTAD prevé que se regirán por sus normas específicas diversos ficheros: los electorales, los relativos a materias clasificadas, los del

Registro Civil y del Registro Central de Penados y Rebeldes, los estadísticos, y los relativos al personal militar profesional (art. 2. 3). El art. 2.1 del R.D. 1332/1994 reitera esta sujeción a regímenes especiales.

Por otro lado, los arts. 40 y 41 LORTAD permiten que, en forma parcial, queden fuera de su ámbito de aplicación y del control de la APD los ficheros públicos creados por las Comunidades Autónomas. El reparto de competencias entre Estado y Comunidades Autónomas en esta materia está pendiente de concreción por el Tribunal Constitucional.

## 2. El régimen general de la creación de ficheros de datos

Sobre el responsable del fichero de datos pesan una serie de deberes y obligaciones para garantizar la exactitud de los datos recogidos, la voluntariedad en la prestación de esos datos por los afectados, y la seguridad y secreto de los datos obtenidos.

Así, para garantizar su exactitud la Ley exige que los datos sean exactos y estén puestos al día; que no se utilicen para fines distintos de los recogidos; que sean cancelados los datos cuando ya no sean necesarios; y se prohíbe la recogida de datos por medios ilícitos o fraudulentos (art. 4). No obstante, remite a un desarrollo reglamentario el procedimiento para mantener «*íntegro determinados datos*» «*atendidos sus valores históricos*» (art. 4.5).

Para garantizar la voluntariedad en la prestación de los datos, la Ley establece que se informe al afectado de la existencia del fichero y de su finalidad, de la identidad y dirección del responsable del fichero, y de la posibilidad de ejercitar sus derechos de acceso, rectificación y cancelación (art. 5). De nuevo la Ley da una de arena, pues esta información no es necesaria si la misma «*se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban*» (art. 5.3). Pensemos en la recogida de datos personales con ocasión de la antigua elaboración de los censos municipales, base para los censos electorales y pieza codiciada por delincuentes y oportunistas; o en las numerosas promociones comerciales (v.gr.: regalos, concursos, sorteos, descuentos, etc.) realizadas por empresas cuyo objetivo último es obtener los datos personales del consumidor o usuario de ciertos bienes y servicios.

Para la recogida de los datos se requiere el consentimiento del afectado

(art. 6), principio medular que, luego veremos, en la práctica queda desvirtuado ante los ficheros más molestos, como son los creados con fines de publicidad comercial o no comercial (pues la Ley no aclara) o los polémicos ficheros sobre morosidad o solvencia patrimonial. No obstante, entre los principios básicos de la Ley ya figura la excepción, este consentimiento no es preciso cuando estemos ante datos de carácter personal procedentes de «fuentes accesibles al público» (art. 6.2). Lo inconcreto del concepto jurídico es evidente (¿tienen este carácter la información de los censos municipales personales y de solares, los registros de instituciones religiosas, los registros o bases de datos de centros sanitarios o educativos, los asientos del Registro de la Propiedad o del Registro Mercantil, o del Registro de Cooperativas o de la Oficina Española de Patentes y Marcas, y las informaciones de los innumerables Registros administrativos sectoriales que proliferan en nuestro Ordenamiento jurídico). El citado art. 1.3 R.D. 1332/1994 no despeja las dudas con su alusión a «cualquier norma limitativa» (v. *supra*). Tampoco es necesario el consentimiento cuando los datos «se recojan para el ejercicio de las funciones propias de las Administraciones Públicas». ¿Cabe mayor imprecisión jurídica y mayor discrecionalidad administrativa? Además de los reparos de constitucionalidad que suscitan, estas excepciones desvirtúan los principios del art. 4 sobre la calidad de los datos.

Por su parte, para determinada información especialmente sensible se establece un régimen más riguroso. En efecto, para recoger datos que revelen la ideología, religión o creencias de las personas se exige el consentimiento «expreso y por escrito del afectado», y se prohíbe crear ficheros cuya sola finalidad sea almacenar datos «que revelen la ideología, religión, creencias, origen racial o vida sexual» (art. 7). No obstante, como siempre la Ley deja el portillo abierto a la discrecionalidad normativa y administrativa, pues permite la creación de estos ficheros y su tratamiento y cesión «cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente» (art. 7.3). Recordemos que esta apelación al interés general tiene un límite infranqueable, el representado por el art. 16.2 CE cuando establece que «Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias».

Para garantizar la seguridad y secreto de los datos recabados se establecen dos previsiones: 1º) el responsable del fichero debe adoptar las medidas

necesarias para garantizar la seguridad de los datos, su alteración y el acceso no autorizado a ellos (art. 9); 2º) este mismo responsable debe guardar secreto profesional sobre los datos recogidos y su tratamiento (art. 10).

Por último, la Ley aborda la delicada cuestión de la cesión de datos de carácter personal. Singularmente estas operaciones de interconexión de datos personales de distintas fuentes son las que permiten crear ese perfil personal del que se pueden derivar consecuencias discriminatorias y nocivas para los ciudadanos. Como regla esta cesión sólo es posible para cumplir los fines a los que legítimamente se dediquen cedente y cesionario, y exige el previo consentimiento del afectado, consentimiento que debe ser concreto (para un cesionario determinado o determinable y constando la finalidad) y es revocable (art. 11). Ahora bien, la Ley enumera un extensa lista de salvedades a esta necesidad de consentimiento: previsión de una Ley; datos recogidos en fuentes accesibles al público; ficheros que ya prevean la posible cesión (excepción peligrosísima, pues equivale a un consentimiento previo y en el vacío); cuando los destinatarios sean el Defensor del Pueblo, el Ministerio Fiscal, o la Judicatura; cesión entre Administraciones Públicas para el ejercicio de las mismas competencias o con destino a otras Administraciones Públicas (de nuevo la discrecionalidad administrativa); o datos relativos a la salud por razones de urgencia o para estudios epidemiológicos (art. 11.2). La propia Ley recorta algo esta anulación del consentimiento, cuando establece que en el supuesto de datos procedentes de fuentes accesibles al público la cesión «no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa» (art. 19.3).

A pocos se oculta que si la regulación de la cesión de datos personales en un contexto nacional es delicada, se convierte en una tarea sumamente compleja y problemática cuando nos trasladamos a las relaciones internacionales. Cuando la cesión o transferencia de datos personales tenga como destinatario otro Estado, la LORTAD exige que el país en cuestión tenga un nivel de protección equiparable al español. En otro caso, se exige el cumplimiento de la Ley española y autorización previa de la APD, cuyo Director sólo podrá acordarla si se obtienen las adecuadas garantías (v. art. 32 LORTAD y 3 R.D. 1332/1994). No obstante, esta autorización no es necesaria en diversos supuestos de transferencia internacional: aplicación de Tratados internacionales; transferencias con finalidad de auxilio judicial internacional; por motivos sanitarios; y transferencias

dinerarias según su legislación específica (art. 33 LORTAD y su desarrollo en el art. 4 R.D. 1332/1994). El régimen jurídico de las transferencias internacionales de datos personales es bastante simple y claro, si bien los nuevos hechos lo han dejado anticuado, cuando no claramente en ridículo. Hoy por hoy son muchos los usuarios de *internet* que pueden acceder a numerosos archivos (actividad para la que –supongamos– están autorizados) y transferirlos por correo electrónico a otro usuario en distinto país (actividad que por el contenido de la información –supongamos– exigía control o autorización administrativa y la Administración ignora la transferencia), sin ningún problema técnico ni cortapisa legal. Las normas sobre protección de las transferencias internacionales de datos personales no están ideadas para un espacio como *internet* que, por estructura y funcionamiento, es refractario a controles y límites. Sin duda, del buen o mal uso de *internet* dependerá que la opinión pública presione para que se creen e introduzcan controles en este medio de comunicación mundial.

### 3. Los derechos de los afectados

Como es tradicional en la legislación comparada sobre protección de datos personales sometidos a procedimientos informáticos, y en el Convenio 108 del Consejo de Europa (v. su art. 8), la LORTAD reconoce y regula los (*sic*) «Derechos de las personas» (arts. 12 a 17), que son desarrollados por los artículos 11 y ss. del R.D. 1332/1994. La Exposición de motivos de la LORTAD avanza que estos derechos «otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático». Con carácter fundamental se reconocen tres derechos:

- 1º) Derecho de información: cualquier persona tiene derecho a conocer la existencia de ficheros automatizados, sus fines y el responsable del fichero. Para ello se debe acudir al Registro General de Protección de Datos que depende de la Agencia de Protección de Datos. Esta consulta es gratuita (art. 13).
- 2º) Derecho de acceso (o, *habeas data*): el afectado tiene derecho a obtener información de sus datos de carácter personal incluidos en los ficheros automatizados. Esta información puede consistir en la visualización del

fichero o en la comunicación por escrito, sin que puedan utilizarse claves o códigos que exijan dispositivos específicos para su empleo. La Ley prevé que, salvo que exista un interés legítimo, este derecho puede ser ejercitado en intervalos no inferiores a doce meses (art. 14). Según el R.D. 1332/1994 para el ejercicio de este derecho de acceso basta la solicitud dirigida al responsable del fichero. La información suministrada por este responsable será legible e inteligible, y abarcará los datos de base y los resultantes de su tratamiento informático, el origen de los datos, los cesionarios de los mismos, y las finalidades y usos para las que se han almacenado.

- 3º) Derecho de rectificación y cancelación: su regulación se deja en manos de futuros Reglamentos. No obstante, la Ley prevé que los datos inexactos o incompletos serán rectificadas o cancelados en su caso, sin que se pueda pedir ninguna contraprestación (art. 15). El R.D. 1332/1994 procede a este desarrollo normativo. Si el afectado constata la existencia de datos «*inexactos o incompletos, inadecuados o excesivos*» puede solicitar del responsable del fichero la oportuna rectificación o, en su caso, la cancelación, que debe hacerse efectiva en el plazo de cinco días (art. 15.1 y 2). Si por razones técnicas la cancelación de los datos no es procedente, el responsable del fichero debe proceder al bloqueo de los datos, para impedir su posterior empleo. Es más, si los datos han sido obtenidos en forma fraudulenta, desleal o ilícita la cancelación comportará la destrucción del soporte del fichero (art. 16).

Los derechos de acceso y de rectificación y cancelación son personalísimos, y serán ejercidos por el afectado frente al responsable del fichero. No obstante, también podrá actuar el representante legal cuando el afectado esté en situación de incapacidad o de minoría legal que le impida el ejercicio de estos derechos (art. 11 R.D. 1332/1994).

Juntos a los anteriores derechos fundamentales, la LORTAD contempla otros dos con un carácter tutelar y reparador. Así, la Ley prevé que los afectados tienen derecho a ser indemnizados por los daños y perjuicios que sufran en sus bienes o persona como consecuencia de incumplir el responsable del fichero las previsiones legales (art. 17). Y, por otro lado, la Ley permite impugnar tanto los actos administrativos como las decisiones privadas que supongan una valoración del comportamiento de una persona que se base sólo en el tratamiento de datos

automatizados que ofrezcan una definición de sus características o personalidad (art. 12). Con un carácter más amplio, el R.D. 1332/1994 legitima a los afectados para que puedan recurrir ante la APD cuando consideren vulneradas las previsiones de la LORTAD, especialmente en lo relativo al ejercicio de sus derechos frente a los responsables de los ficheros. Se establece un procedimiento sumario ante la propia APD cuya resolución se comunica a los interesados, y es susceptible de recurso contencioso-administrativo (art. 17).

#### *4. Las normas especiales para los ficheros de titularidad pública y los de titularidad privada*

En el caso de ficheros de titularidad pública su mayor singularidad consiste en que su creación, modificación o supresión sólo puede hacerse mediante una disposición general publicada en el BOE o en el diario oficial correspondiente (v., por ejemplo, la Resolución de la Dirección de la APD de 18 de julio de 1994 por la que se regulan los ficheros automatizados de datos de carácter personal existentes en la propia Agencia, BOE núm. 180, del 29 de julio; o la Resolución de la Comisión del Sistema Eléctrico Nacional de 17 de diciembre de 1996, BOE núm. 27, de 31 de enero de 1997). La LORTAD indica el contenido de estas disposiciones (art. 18); y el R.D. 1332/1994 exige la notificación de los ficheros públicos a la APD y su inscripción en el Registro General de Protección de Datos. Por su parte, la cesión de datos tiene que estar prevista en esta norma o en otra de rango superior (art.19).

Por otro lado, como permite la legislación comparada –pero en forma más concreta y restrictiva– se establece una regulación especial para los ficheros de las fuerzas y cuerpos de seguridad (arts. 20 a 22). En ella se contienen numerosas e importantes excepciones a los derechos de acceso y rectificación y cancelación de los afectados, y no sólo en aras de la defensa del Estado, la seguridad pública o la protección de los derechos y libertades –como contempla el Convenio 108–, sino también en el caso de otros ficheros. Por ejemplo, en estos tres supuestos: 1º) para los fines propios de la Hacienda Pública (v. art. 21.2; y Resolución de la Agencia Estatal de la Administración Tributaria de 29 de noviembre de 1996, sobre instrucciones relativas al acceso a sus bases de datos, BOE núm. 306, de 20 de diciembre); 2º) para las «necesidades de las investigaciones que se estén realizando»; y 3º) para «el cumplimiento de las

*funciones de control y verificación de las Administraciones Públicas».* Muchos de estos recortes a los derechos cívicos suscitan serias dudas de constitucionalidad.

Respecto a los ficheros de titularidad privada la Ley permite que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona o empresa titular del fichero y se respeten las previsiones de esta Ley (art. 23).

Se exige que el titular del fichero lo comunique a la Agencia de Protección de Datos, con todos los requisitos establecidos por la ley, y el fichero se inscribirá en el Registro General de Protección de Datos (art. 24). Los pormenores de estas actuaciones han sido remitidos al desarrollo reglamentario operado por R.D. 1332/1994 (arts. 6 a 10, y véase también la Resolución APD de 22 junio de 1994 por la que se aprueban los modelos normalizados para efectuar las correspondientes inscripciones, BOE núm. 149, de 23 de junio). Por su parte, la LORTAD —como hace el Convenio del Consejo de Europa— estimula a los responsables de estos ficheros para que aprueben normas deontológicas reguladoras de los ficheros de titularidad privada, normas que deben ser depositadas en el Registro General de Protección de Datos, si se ajustan a las normas legales y reglamentarias sobre la materia (art. 31).

Con relación al delicado tema de la cesión de datos, la LORTAD exige al responsable del fichero privado que, como regla, cuando efectúe la primera cesión informe de ello a los afectados, indicando la finalidad del fichero, los datos cedidos y la identificación del cesionario (art. 25). Esta obligación se excepciona cuando la cesión venga impuesta por Ley, o cuando el destinatario sea el Defensor del Pueblo, el Ministerio Fiscal o la Magistratura. A estas excepciones se adicionan dos más que convierten a esta obligación, en muchos casos, en un mero *brindis al sol*, se trata de la cesión entre Administraciones Públicas (v.gr.: la noticia de que el Ayuntamiento de Granada pretende cruzar los datos del padrón con los de Sevillana de Electricidad para aumentar la recaudación fiscal, v. Diario *El País*, de 28 de marzo de 1996), y cuando estemos ante ficheros que prevén su interconexión con otros de terceros (v.gr.: comunicación de Telefónica a todos sus abonados de que sus datos pueden ser intercambiados con sus filiales y con empresas participadas por el Grupo Telefónica, «salvo instrucciones expresas en contrario» por parte de los abonados).

Junto a estas previsiones generales, la LORTAD contiene algunas normas

referidas a ficheros privados de determinadas características. Veamos:

- A) Datos sobre abonados a servicios de telecomunicaciones: el afectado puede exigir su exclusión de los repertorios de abonados de acceso al público (art. 26).
- B) Empresarios dedicados a prestar el servicio de tratamiento automatizado de datos de carácter personal: no pueden emplearlos para fines distintos de los que figuren en el contrato de servicio, ni cederlos a otras personas. Deben destruir los datos una vez cumplido el contrato, salvo autorización de la contraparte o si se presume que van a ser necesarios para posteriores relaciones contractuales (art. 27).
- C) Prestación de servicios de información sobre solvencia patrimonial y crédito: quienes se dediquen a prestar estos servicios sólo pueden tratar datos obtenidos de fuentes accesibles al público o de informaciones facilitadas por el afectado o con su consentimiento. Para evitar reiteraciones, véase *infra* el comentario a este respecto. También pueden tratar datos que aporten acreedores sobre cumplimiento o incumplimiento de obligaciones dinerarias, si bien, en este caso hay que informar al afectado. Por su parte, el afectado puede solicitar la información que exista sobre él, así como a quién se ha cedido. Y, se establece un límite temporal: sólo se pueden tratar y ceder estos datos para enjuiciar la solvencia patrimonial, si son adversos, en los seis últimos años (art. 28). Con datos de 1995, el 40 por 100 de las 10.000 consultas realizadas por los españoles a la APD tenían que ver con la morosidad (v. Diario *El País* de 21 de mayo de 1996). No es de extrañar que la primera Instrucción dictada por la APD en 1995 haya venido a desarrollar el art. 28 LORTAD, y en unos términos que han gustado poco a la Asociación Nacional de Entidades de Financiación (ASNEF) que ha recurrido la Instrucción ante la jurisdicción contencioso-administrativa, y desde diversos foros la combate por activa y por pasiva mediante sus asesores legales (v., como ejemplos de estos ataques, Muñoz Gutiérrez, 1996, 11-14; y, Alonso Martínez, 1996, 1 y 4-10).
- D) Ficheros con fines de publicidad: sólo se pueden tratar los datos que figuren en fuentes accesibles al público, o cuando los datos hayan sido facilitados por los afectados u obtenidos con su consentimiento. Por su parte, los afectados tienen derecho a conocer el origen de sus datos, así

como a darse de baja inmediatamente en el fichero, cancelándose sus datos mediante una simple solicitud (art. 29). En estos ficheros, como en los de solvencia patrimonial, el principio de consentimiento del afectado resulta desvirtuado, así como el principio de calidad de los datos recabados. No hay consentimiento si estamos ante una fuente accesible al público. Este carácter público a ciertos efectos, no implica autorización o consentimiento para su utilización con fines de publicidad comercial o para enjuiciar la solvencia patrimonial. El mismo argumento puede esgrimirse para los datos recogidos con el consentimiento del afectado, pero para fines diversos. En esta sede el legislador vuelca sobre las espaldas del consumidor y usuario con el peso de destruir esa presunción de consentimiento, obligándole a recabar la información existente y solicitar la cancelación de los datos personales que consten sobre él. Y todo, en el supuesto de que las previsiones legales sean realmente eficaces, y no nos encontremos —como ha evidenciado la práctica— ante negligencias y abusos informáticos que eternicen en ciertas bases los datos erróneos, inexactos o recabados ilícitamente de multitud de ciudadanos (v. las denuncias de la Asociación de Usuarios de Servicios Bancarios —AUSBANC— en Diario *Cinco Días*, de 10 de octubre de 1997).

##### 5. *Las infracciones y sanciones administrativas*

La última parte de la Ley (arts. 42 a 48) regula las infracciones y sanciones administrativas a las que están sujetos los responsables de los ficheros.

Como exige la jurisprudencia constitucional, el legislador tipifica un amplio conjunto de infracciones leves, graves y muy graves que se concretan en incumplimientos de la LORTAD (v. art. 43).

Por su parte, respecto a las sanciones, para los ficheros de titularidad privada se prevé la sanción de multa que puede ir desde 100.000 a 10.000.000 ptas. para las infracciones leves, a una multa de 50 a 100 millones de ptas. para las infracciones muy graves (art. 44). En el caso de ficheros de titularidad pública, la APD exigirá las medidas oportunas para que cese la infracción, y se exijan las oportunas responsabilidades disciplinarias (art. 45). Por otro lado, para ambos tipos de ficheros se establece que

para infracciones muy graves que atenten contra los derechos de los ciudadanos, el Director de la Agencia puede requerir la cesación en la utilización o cesión ilícita de los datos. Si este requerimiento es desatendido, la Agencia puede inmovilizar el fichero en cuestión (art. 48).

El procedimiento sancionador fue remitido a un ulterior desarrollo reglamentario (art. 47), que ha tenido lugar en el citado R.D. 1332/1994. Este procedimiento se ventila ante la APD, cuyo Director nombra un instructor, y la resolución del Director de la APD es recurrible ante la jurisdicción contencioso-administrativa (arts. 18 y 19).

Conviene advertir que en el nuevo Código Penal (Ley Orgánica 10/1995, de 23 de noviembre) ya se establecen algunos tipos delictivos donde se tutelan los datos de carácter personal contenidos en soportes informáticos frente al descubrimiento de secretos o la vulneración de la intimidad (art. 197). Si bien, no se tipifican directamente como delito las violaciones al derecho de libertad informática.

#### IV. La Agencia de Protección de Datos

La LORTAD crea la Agencia de Protección de Datos como órgano encargado de velar por el cumplimiento de sus previsiones. Su estatuto sería aprobado por el Gobierno (art. 34.2), y está contenido en el citado Real Decreto 428/1993, de 26 de marzo, recientemente reformado para adicionarle un nuevo apartado a su art. 9 que designa a la APD como Representante español a los efectos del art. 29 de la Directiva 95/46/CE, de 24 de octubre.

La Ley configura la APD como un Ente de Derecho Público con personalidad jurídica propia, al que se adscriben una serie de medios personales (funcionarios o personal contratado, según las funciones) y materiales (la Agencia elabora el Anteproyecto de Presupuesto anual y lo remite al Gobierno para su aprobación, con la debida independencia, en los Presupuestos Generales del Estado). La Ley, tanto en su Exposición de motivos como en su articulado, subraya la independencia y objetividad de sus actuaciones —«*actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones*» (art. 34.3), su Director ejerce «*sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas*» (art. 35.2)—; pero, en las normas y en la práctica, el eje de la APD,

que es su Director, lo nombra el Gobierno mediante Real Decreto entre los miembros del Consejo Consultivo, y puede cesarlo el propio Gobierno, previo expediente donde serán «oídos» los restantes miembros del Consejo Consultivo «*por incumplimiento grave de sus obligaciones*» (art. 35. 1 y 3). Estamos lejos de una figura similar a la de un Defensor del Pueblo en materia informática (v., en términos rotundos Pérez Luño, 1996, 56; y muy matizadamente De la Serna Bilbao, M<sup>a</sup>. N., 1997, 12–14), y no podemos dejar de insistir en que los derechos de los ciudadanos son tales si realmente se arbitran procedimientos eficaces para su cumplimiento (Paniagua Zurera, 1992, 10).

La APD ejerce sus funciones a través del Director, cuyos actos –que agotan la vía administrativa– se consideran actos de la Agencia (art 35.1 LORTAD y art. 1.3 R.D. 428/1993). La LORTAD y su desarrollo reglamentario contienen el estatuto jurídico del Director en cuanto a duración del mandato (cuatro años), causas de cese (se limitan a la incapacidad sobrevenida, la incompatibilidad, la condena por delito doloso y, la ya adelantada, el incumplimiento grave de las obligaciones de su cargo), incompatibilidades (las propias de los altos cargos), y remuneración (la correspondiente a los subsecretarios).

Junto al Director, como figura clave, conforman la APD el Consejo Consultivo y el Registro General de Protección de Datos. A los que el R.D. 428/1993 adiciona la Inspección de Datos y la Secretaría General.

El Consejo Consultivo asesora al Director de la Agencia a través de sus informes y propuestas, y tiene una composición dispar y plural: un Diputado, un Senador, un Representante de la Administración del Estado, otro de la Administración Local, otro de la Autonómica, un miembro de la Real Academia de la Historia, un experto en la materia propuesto por el Consejo Superior de Universidades, un Representante de los consumidores y usuarios, y un Representante del «*sector de ficheros privados*» (art. 37 LORTAD y art. 19 R.D. 428/1993). Su funcionamiento lo remite la LORTAD a un ulterior desarrollo reglamentario (v. arts. 20 a 22 R.D. 428/1993).

Por su parte, en el Registro *ad hoc* creado se inscribirán los ficheros de titularidad pública y privada, las autorizaciones previstas en la Ley, los códigos deontológicos que auspicia, y los datos necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación (art. 38). El R.D. 428/1993 pormenoriza esta previsión legal en sus artículos 23 a 26.

La Inspección de Datos es el órgano de la APD que ejerce la potestad de

inspección que compete a la Agencia según el art. 39 LORTAD, y también instruye los expedientes sancionadores donde se contemplen medidas cautelares y provisionales contra responsables de ficheros privados (arts. 27 a 29 R.D. 428/1993). Finalmente, la Secretaría General se encarga de la labor de gestión, documentación, información, etc. necesaria para el eficaz funcionamiento de la APD (arts. 30 y 31 R.D. 428/1993).

La Ley enumera una amplia lista de funciones o competencias de la APD (art. 36 y 39) que, a su vez, han sido pormenorizadas por el R.D. 428/1993. Sin carácter exhaustivo podemos sistematizar las aludidas competencias en la forma siguiente:

- 1º) Competencias normativas o «paranormativas»: dictar instrucciones para adecuar los tratamientos automatizados a los principios de la Ley (Marroig Pol, 1997, 1-10); informar los proyectos de disposiciones generales que desarrollen la Ley; conceder las autorizaciones previstas en la Ley; redactar su memoria anual y remitirla al Ministerio de Justicia; y velar por el cumplimiento de la Ley en el caso de ficheros de titularidad pública o con fines estadísticos.
- 2º) Competencias sancionadoras, cautelares y preventivas: ejercer la potestad sancionadora (De Asís Roig, A. E., 1997, 1-9); ordenar el cese del tratamiento de datos y la cancelación de ficheros que no se ajusten a la Ley; recabar de los responsables de los ficheros la ayuda e información necesaria para cumplir sus funciones; dar publicidad a la existencia de ficheros automatizados publicando periódicamente una relación de los mismos; controlar y autorizar los movimientos internacionales de datos; e inspeccionar los ficheros automatizados y recabar toda la información necesaria.
- 3º) Competencias de servicio al ciudadano: atender las peticiones y reclamaciones formuladas por las personas afectadas; proporcionar información a estas personas sobre sus derechos en esta materia; y controlar la aplicación de la Ley en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.
- 4º) Competencias residuales: las que le sean atribuidas por otras normas legales.

## V. La Directiva comunitaria sobre protección de las personas físicas en lo que respecta al tratamiento automatizado de datos personales y a la libre circulación de estos datos

La Directiva 95/46/CE se viene gestando desde el inicio de la década de los noventa hasta que, por fin, es aprobada el 24 de octubre de 1995 y se publica en el DOCE del 23 de noviembre de ese año (v. DOCE núm. L 281 de 23.11.1995, pp. 31-50). Sin duda la nueva Directiva va a tener un impacto obligado en la LORTAD y sus normas de desarrollo (Martín-Casallo López, 1996, 3-6).

La Directiva 95/46/CE está precedida por una extensa serie de *considerandos* donde se justifica y adelanta parte de su articulado. La Comunidad tiene presente que los sistemas de tratamiento de datos «*están al servicio del hombre*» y deben respetar «*las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad*». Ahora bien, la Comunidad también es consciente de que el mercado interior exige «*la libre circulación de datos personales de un Estado miembro a otro*», que estos flujos transfronterizos experimentarán un «*aumento notable*», y resulta necesario paliar las «*diferencias entre los niveles de protección*». Por ello es preciso que la Comunidad «*intervenga para aproximar las legislaciones*» sin que esta operación conduzca «*a una disminución de la protección*» actual, pues el objetivo es «*asegurar un alto nivel de protección dentro de la Comunidad*».

La Directiva concede a los Estados miembros el plazo de tres años, a partir de su adopción, para introducir las medidas legales necesarias en orden a su cumplimiento. Este plazo general sólo resulta parcialmente excepcionado (se amplía a doce años) para los ficheros manuales existentes a su entrada en vigor (art. 32.1 y 2)

Si seguimos parcialmente el esquema empleado para el análisis de la LORTAD (v. *supra* apartado IV), la Directiva debe tener una incidencia importante en Derecho español en las materias que siguen.

### 1. *Ámbito de aplicación*

La Directiva excluye de la aplicación de sus previsiones las materias siguientes: el tratamiento de datos para actividades domésticas (como la correspondencia o repertorios de direcciones); los datos relativos a la seguridad

publica, defensa, seguridad del Estado y los datos relativos a condenas y penas; los datos necesarios para salvaguardar el bienestar económico cuando este tratamiento esté relacionado por la seguridad del Estado; y los datos relativos a las personas jurídicas (art. 3 y Considerando 24).

El contraste con la LORTAD es evidente en algunos puntos. Numerosas excepciones contenidas en el art. 2 de la Ley española tendrán que ser reexaminadas (v.gr.: ficheros públicos para su publicidad general; ficheros que recojan datos publicados en boletines o diarios oficiales; y ficheros de partidos políticos, sindicatos y confesiones religiosas sobre sus miembros o exmiembros). No obstante, la Directiva permite a los Estados la introducción de diversas excepciones a la prohibición de tratamiento de ciertos datos que pueden afectar a derechos fundamentales o a datos sensibles. Es el supuesto de que estos tratamientos se hagan con fines de salud, protección social, investigación científica, estadísticas públicas, fines periodísticos o de expresión artística o literaria, o cuando el tratamiento se realice por personas físicas sometidas a una obligación legal de secreto profesional o para la legítima actividad de ciertas asociaciones o fundaciones cuyo objeto es posibilitar el ejercicio de las libertades fundamentales. En este punto habrá que tener muy presente si, en la práctica, se consigue el objetivo de no disminuir los actuales niveles nacionales de protección, y elevar los existentes en la Unión Europea.

## 2. Régimen de creación de los ficheros de datos

Las diferencias entre la Ley española y la Directiva comunitaria son ya más matizables. La Directiva contiene previsiones similares a las de la LORTAD con relación a la exactitud de los datos recabados, la voluntariedad en la prestación de los datos, y la seguridad y secreto de los datos obtenidos (arts. 6, 7, 16 y 17). Así, por ejemplo, la Directiva insiste en que los datos deben ser *«adecuados, pertinentes y no excesivos con los fines para los que se recaben y para los que se traten posteriormente»* (art. 6.1 letra c), y que los fines posteriores no pueden ser incompatibles con los originarios (art. 6.1 letra b).

Por otro lado, la Directiva enumera una serie de categorías de datos sensibles: los relativos a origen étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, y los atinentes a la salud o a la vida sexual. Los Estados tienen que prohibir el tratamiento de estos datos (art. 8.1), salvo

cierta excepciones previstas en la propia norma (art. 8.2).

Respecto a la cesión de datos, la Directiva exige que los Estados establezcan excepciones a la transferencia de datos personales a terceros países que no prevean una protección equiparable, incluso autoriza a la Comisión para comprobar la existencia o no de esa garantía (art. 25). No obstante, en esta cuestión se permite a los Estados un amplio margen de maniobra (art. 26).

Hemos de destacar que la Directiva no distingue, como hace la Ley española, entre el régimen jurídico de los ficheros públicos y el de los ficheros privados. Ello no impide establecer un régimen diversificado en función de la distinta titularidad (la propia Directiva admite su recepción tanto mediante una ley general, como mediante leyes sectoriales), lo que sí parece contrario es «*que tal diferenciación suponga de hecho una minoración de los derechos reconocidos al interesado o afectado*» (Martín-Casallo López, 1996, 6). La aplicación de este criterio pone en tela de juicio el contenido del art. 19 LORTAD relativo a la cesión de datos entre Administraciones públicas.

### 3. Los derechos de los ciudadanos

Estos derechos frente al tratamiento automatizado de sus datos de carácter personal son reconocidos por la Directiva en términos similares a los previstos en la legislación española. En efecto, la Directiva reconoce el derecho de información tanto de la recogida de datos, recabados del interesado o no, como de su tratamiento (arts. 10 y 11).

Por otro lado, se reconoce en forma amplia el derecho de acceso para comprobar la exactitud y licitud del tratamiento (art. 12 letra a). Asimismo, se reconocen los derechos de rectificación, supresión o bloqueo de los datos (art. 12 letras b y c). Ahora bien, el art. 13 autoriza a los Estados para establecer excepciones y limitaciones al alcance de estos derechos por motivos que coinciden, *mutatis mutandis*, con las causas de exclusión del ámbito de aplicación de la Directiva.

Como novedad mayor de la Directiva se sitúa la regulación del «*derecho de oposición del interesado*» (art. 14). Supone que los Estados miembros han de reconocer al interesado el derecho a oponerse, al menos en algunos casos, «*en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento*».

Asimismo, el interesado puede oponerse al tratamiento de sus datos personales para fines de prospección. No obstante, como siempre, los Estados pueden establecer excepciones a este derecho. Será el desarrollo normativo nacional el que concrete el contenido de este derecho de oposición (Martín-Casallo López, 1996, 6).

#### 4. *La autoridad de control*

La Directiva considera que la creación de una «*autoridad de control que ejerza sus funciones con plena independencia*» en cada Estado es esencial para la protección de las personas respecto al tratamiento de datos personales (Considerando 62). El art. 28 configura esta autoridad de control mediante el reconocimiento de un amplio abanico de posibilidades de actuación (consulta antes de la aprobación de normas legales; facultades de investigación; facultades de intervención –v. gr.: formulación de dictámenes, ordenes de bloqueo o destrucción de datos; prohibición de tratamiento de datos; y amonestación a las autoridades e instituciones nacionales–; legitimación procesal, etc.), y cada Estado miembro decidirá qué «*autoridades públicas*» se encargarán de ejercer estas competencias. Como adelantamos, en virtud del R.D. 156/1996, la APD ha sido designada como Representante español a los efectos de la presente Directiva. Esta misma norma ha establecido que será el Director de la Agencia el que designe al representante para el Grupo de Protección de las Personas que regula la citada Directiva (arts. 29 y 30), con funciones de asesoramiento a la Comisión europea y de control de la aplicación uniforme de la Directiva en los Estados miembros (De la Serna Bilbao, M<sup>a</sup>. N., 1997, 10–11).

#### 5. *Otras cuestiones*

Finalmente, por su novedad –total o parcial– frente a la Ley española, hemos de comentar los extremos siguientes de la Directiva:

- A) Se contempla el supuesto de datos personales transmitidos a través de servicios de telecomunicaciones o de correo electrónico cuyo objetivo sea transmitir datos de este tipo. Se considera responsable del tratamiento de los datos la persona de quien provenga el mensaje, y el oferente del servicio de transmisión es responsable de los datos personales necesarios

o complementarios para el funcionamiento del servicio (Considerando 47). No podemos olvidar la responsabilidad patrimonial que puede emerger en esta materia.

- B) La Directiva se aplica expresamente a la voz y el sonido como datos personales, con lo que se refuerza la protección de la intimidad personal (Considerandos 14 a 17). El art. 1.4 R.D. 1332/1994 ya recoge una noción amplia de la expresión «*datos de carácter personal*». Por su actualidad entre nosotros, hay que advertir que el supuesto de la vigilancia por videocámaras no está comprendido en el ámbito de aplicación de la Directiva cuando se aplica a fines de seguridad pública, defensa, seguridad del Estado, o la aplicación del Derecho penal.

En fecha reciente el Estado español ha regulado —en cierta medida espoleado por los dramáticos hechos delictivos del terrorismo y de la delincuencia organizada— la utilización por las fuerzas y cuerpos de seguridad del Estado de videocámaras y otros medios técnicos para grabar imágenes y sonidos en lugares públicos y el posterior tratamiento de estos datos. En efecto, la Ley Orgánica 4/1997, de 4 de agosto (BOE núm. 186, del 5) establece la mencionada regulación, así como las garantías para los derechos fundamentales de los ciudadanos, especialmente, los derechos al honor, a la intimidad personal y familiar, a la propia imagen y, por extensión, a la libertad informática. En este sentido, la Ley dispone que el tratamiento automatizado de las imágenes y sonidos recabados se regirá, además de por sus normas, por las de la LORTAD (art. 2.2); asimismo la LORTAD se aplica a los datos captados por videocámaras con fines de control del tráfico viario (Disposición adicional octava L.O. 4/1997). El art. 9 de la Ley contempla los «*derechos de los interesados*» que, como avanza la Exposición de motivos, se concretan en dos: 1º) derecho del público a ser informado de manera clara y permanente de la existencia de videocámaras fijas, «*sin especificar su emplazamiento*», y de quién es la autoridad responsable; 2º) derecho de toda persona interesada a tener acceso a las grabaciones en que razonablemente considere que figura, y derecho de cancelación, el ejercicio de estos últimos derechos puede «*ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad públi-*

ca, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando». Se remite a un ulterior desarrollo reglamentario la determinación del «*órgano o autoridad gubernativa*» competente para resolver sobre las peticiones de acceso o cancelación (art. 8.4). Por otro lado, la Ley establece la destrucción de los datos recogidos «*en el plazo máximo de un mes desde su captación*» y prohíbe «*la cesión o copia de las imágenes y sonidos obtenidos*» salvo, en ambos supuestos, que las grabaciones «*estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto*» (art. 8.1 y 3). Como podemos advertir las previsiones reproducidas introducen una importante dosis de discrecionalidad administrativa, la propia Ley parece haber querido poner el *parche* antes de que surja la *herida*, cuando reitera el deber de «*reserva, confidencialidad y sigilo*» que pesa sobre las personas que, por razón de sus funciones, tienen acceso a estas grabaciones (art. 8.2), y recuerda que las infracciones a esta Ley pueden estar tipificadas como delito o como infracción administrativa, en cuyo caso se hacen acreedoras de las sanciones generales previstas en el régimen disciplinario y, en su defecto, las sanciones recogidas en la LORTAD (art. 10). Finalmente hay que reseñar que contra las resoluciones administrativas dictadas en aplicación de esta Ley cabe la interposición de recursos administrativos, del recurso ante la jurisdicción contencioso-administrativa y, lo que es más interesante, de los recursos «*previstos en el artículo 53.2 de la Constitución*» (art. 11), es decir, los procedimientos preferentes y sumarios ya mencionados (v. *supra* Apartado II) y, por supuesto, la vía del recurso de amparo.

- C) La Directiva va a obligar a redimensionar las relaciones entre el derecho a la intimidad y la libertad de expresión, pues permite el tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, y los Estados sólo podrán establecer excepciones cuando resulten necesarias para conciliar el derecho a la intimidad con las normas reguladoras de la libertad de expresión (art. 9) (v. como primeras reacciones, Betés de Toro, 1997, 6-10). A este efecto habrá que tener

muy presente la doctrina del Tribunal Constitucional que, tras una primera etapa donde cuestiona la posición prevalente del derecho al honor y a la intimidad, ha establecido la posición preeminente de la libertad de información y la interpretación restrictiva del derecho a la intimidad como límite a la libertad de expresión (Espinar Vicente, 1992, 46 y ss.; López Díaz, 1996, 157; y, con matices respecto al derecho al honor, Bustos Pueche, 1992, 101 y ss.). Aunque la delimitación entre estos derechos ha de hacerse caso a caso (v. STS de 24 de julio de 1997, R.A. 5765).

- D) La Directiva debe afectar, asimismo, a otro de los *talones de Aquiles* de la LORTAD: los medios jurisdiccionales que tienen los ciudadanos frente a las violaciones a su derecho a la libertad informática. Hoy estas medidas se concretan, en el marco específico de la normativa de protección frente al tratamiento de datos personales, en el recurso ante la APD y, en su caso, la vía contencioso-administrativa. Posibilidad esta última de dudoso efecto tuitivo, ante la preeminencia de la Administración Pública en su seno. El art. 22 exige a los Estados miembros la introducción, antes del posible recurso administrativo, *«de un recurso judicial en caso de violación de los derechos»* que reconozca la legislación nacional. Esta norma puede ser aprovechada para replantear la conveniencia de que sea la jurisdicción contencioso-administrativa, y no la ordinaria, la que tutele los derechos fundamentales en juego, al menos, cuando estemos ante ficheros de titularidad privada.
- E) La Directiva aborda la responsabilidad por daños en que pueden incurrir los responsables del tratamiento ilícito de datos personales (art. 23), con la singularidad de que esta responsabilidad se configura como subjetiva pero con inversión de la carga de la prueba. Es decir, el responsable del tratamiento puede eximirse total o parcialmente de responsabilidad *«si demuestra que no se le puede imputar el hecho que ha provocado el daño»*.

## VI. A modo de recapitulación crítica

Todas las revoluciones tienen sus luces y sus sombras. Como otras profundas mutaciones históricas, las innovaciones en la tecnología aplicada a la creación, almacenamiento y transmisión de información, se han ido produciendo paulati-

namente, a modo de simple moda pasajera objeto de comentarios distendidos; pero hoy, cuando arañamos un nuevo milenio, y almorzamos con noticias de catástrofes y genocidios junto a descubrimientos médicos e imágenes inéditas de otros planetas, basta pensar en las actividades más cotidianas (v.gr.: adquisición de alimentos y otros suministros esenciales, cobro del salario, asistencia sanitaria, realización de un paseo por un lugar público o de un viaje, incontables procesos productivos, etc.) para advertir que la era de la información no es un anuncio futurista, sino una realidad en expansión.

A nadie se ocultan los beneficios que los avances informáticos han aportado –y seguirán aportando–, sin embargo –y conviene reparar en la paradoja– los nuevos y potentes ordenadores y las nuevas formas de telecomunicación también tienen sus desventajas (¿quién tiene acceso a ellos?, ¿a quién sirven?, ¿quién los controla?, ¿nos hacen más iguales?, ¿más libres?, etc.). Estas cuestiones tienen un profundo calado y algún día se deberán abordar. Pero nuestro propósito es mucho más limitado: hemos analizado el desarrollo legal del derecho de libertad informática. Derecho éste de contornos aún imprecisos, de discutida ubicación y caracterización jurídica (¿nuevo derecho fundamental o mera facultad del derecho a la intimidad?); pero de creciente actualidad. Es más, no debe sorprendernos que, en un futuro no muy lejano, las intromisiones informáticas en la vida de los ciudadanos cobren una magnitud que obligará al Derecho penal a intervenir en forma más intensa. Y, como ocurre con la denominada delincuencia de *cuello blanco*, la tarea no será fácil ante medios tan potentes como *internet* que, por su propio diseño, no conoce ni quiere controles ni límites.

En espera de estos nuevos hechos, el jurista debe enjuiciar críticamente la realidad y la normación vigente. En esta tarea si juzgamos la Norma fundamental advertimos que el legislador constitucional intuyó, más que comprendió cabalmente, el riesgo de la informática para los derechos y libertades fundamentales de los ciudadanos. De ahí que, a modo de apostilla o coletilla reguladora del derecho al honor y a la intimidad, remitiese a la Ley la tutela de los derechos constitucionales frente al uso de la informática (art. 18.4 CE). No obstante esta parquedad normativa, la alusión constitucional tiene una gran *potencialidad normativa* pues –como consecuencias más notables– exige que las normas reguladoras de la libertad informática tengan el rango de Ley orgánica, respeten el *contenido esencial* del art. 18.4 CE, y tienen abiertas las puertas del recurso

de amparo. El encargado de velar por estas garantías es el Tribunal Constitucional que —como sabemos— tiene pendiente el juicio de constitucionalidad sobre la LORTAD. Esperemos que en esta ocasión no ocurra como en otros temas, y el Tribunal Constitucional no se limite a delimitar las competencias entre Estado y Comunidades Autónomas, sino que entre a juzgar la constitucionalidad de las numerosas excepciones previstas en la LORTAD sobre ficheros y datos a los que no se aplican sus normas y, de paso, analice si el contenido de los desarrollos reglamentarios de la LORTAD es o no excesivo por vulnerar el principio de reserva material de ley, y también se pronuncie sobre la atribución a la jurisdicción contencioso-administrativa de los conflictos suscitados por toda la problemática del tratamiento automatizado de datos personales.

El salto de la Norma fundamental a la legislación de desarrollo, en parte ya anticipado, evidencia que al legislador parece preocuparle poco —al menos en un primer momento— el derecho de libertad informática. La LORTAD era necesaria para que el Estado español pudiese cumplir las exigencias al respecto del Acuerdo (policial) de Schengen. No debe extrañarnos, peor fue la historia legislativa de la Ley 24/1984, de defensa de los consumidores y usuarios, cuyo desencadenante último fue el denominado —eufemísticamente— *síndrome tóxico* (Paniagua Zurera, 1992, 46). La inspiración se toma, en principio, del Convenio del Consejo de Europa de 1981 (citado en la propia Exposición de motivos de la LORTAD), pero con importantes y serias *sombras* que, para evitar reiteraciones, pueden enumerarse en las siguientes: 1º) continuas excepciones a sus normas protectoras; 2º) remisiones a legislaciones específicas y a normas reglamentarias de desarrollo; 3º) dudosa imparcialidad del organismo de control (Agencia de Protección de Datos); 4º) el problema —siempre arduo— del reparto de competencias entre Estado y Comunidades Autónomas; 5º) el consentimiento del ciudadano es obviado en numerosos casos; 6º) el delicado tema de la cesión de datos se *despacha* con una norma general, plagada de excepciones; 7º) la distinción entre ficheros de titularidad pública y privada tiene ecos de *«ley de embudo»*, donde la LORTAD habilita a la Administración pública para *saltarse* muchas de sus previsiones; 8º) la práctica diaria pone en tela de juicio el cumplimiento por los titulares de ficheros privados de la LORTAD y la actividad inspectora y sancionadora de la APD (¿qué ciudadano recuerda que una empresa de publicidad, que invade diariamente su correspondencia postal, le haya comunicado que obtuvo los datos en virtud de tal o cual cesión?, ¿cuántas

gestiones son precisas para que un ciudadano, incluido indebidamente en un fichero de morosos, vea cancelados sus datos sobre solvencia patrimonial?, etc.).

Finalmente, la Directiva 95/46/CE se ha quedado muy corta. Sus considerandos y su articulado llevan al lector a la extenuación, no por lo casuístico de la regulación, sino por las amplias facultades que continuamente concede a los Estados para excepcionar o para separarse de las líneas generales que sienta como contenido normativo normal. No obstante, ha de suponer —es de esperar— una mejora de la LORTAD en aspectos como su ámbito de aplicación, la responsabilidad por daños ante tratamientos ilícitos de datos personales, y la homogeneización de las exigencias para ficheros de titularidad pública o privada. Por otro lado, a la hora de su recepción suscitarán problemas, como mínimo, tres temas: 1º) la regulación del derecho de oposición; 2º) la coordinación de la libertad informática con la libertad de expresión; y, 3º) la jurisdicción competente en materia de libertad informática.

### Bibliografía

- ALONSO MARTÍNEZ, C. (1996), Prestación de servicios de información sobre solvencia patrimonial y crédito, *Actualidad Informática Aranzadi*, nº 18, pp. 1 y 4–10.
- BETÉS DE TORO, A. (1997), El derecho de información y los principios legitimadores del tratamiento automatizado de los datos de carácter personal en la Directiva 95/46/CE, de 24 de octubre de 1995, *Actualidad Informática Aranzadi*, nº 25, pp. 6–10.
- BUSTOS PUECHE, J. E. (1992), Los límites de los derechos de libre expresión e información según la jurisprudencia, *Estudios sobre el derecho a la intimidad*, Ed. Tecnos, Madrid, pp. 101–156.
- DE ASÍS ROIG, A. E. (1997), La actividad sancionadora de la Agencia de Protección de Datos, *Actualidad Informática Aranzadi*, nº 22, pp. 1–9.
- DE LA SERNA BILBAO, M<sup>a</sup>. N. (1997), La Agencia de Protección de Datos española: con especial referencia a su característica de independiente, *Actualidad Informática Aranzadi*, nº 22, pp. 10–15.
- DÍEZ-PICAZO, L. y GULLÓN, A. (1995), *Instituciones de Derecho Civil*, I, Ed. Tecnos, Madrid.
- ESPINAR VICENTE, J. M<sup>a</sup>. (1992), La primacía del derecho a la información sobre

- la intimidad y el honor, *Estudios sobre el derecho a la intimidad*, Ed. Tecnos, Madrid, pp. 46-67.
- FERNÁNDEZ CALVO, R. (1993), Datos personales: tecnología, ley y ética, *Actualidad Informática Aranzadi*, nº 8, pp. 1 y 4.
- HEREDERO HIGUERAS, M. (1992), La protección de los datos personales registrados en soportes informáticos. Visión general, *Actualidad Informática Aranzadi*, nº 2, pp. 1-3.
- LÓPEZ-IBOR MAYOR, V. (1993), Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos (LORTAD), *Actualidad Jurídica Aranzadi*, nº 8, pp. 1-4.
- LÓPEZ DÍAZ, E. (1996), *El derecho al honor y el derecho a la intimidad. Jurisprudencia y doctrina*, Ed. Dykinson, Madrid.
- MARROIG POL, L. (1997), Las instrucciones de la Agencia de Protección de Datos, *Actualidad Informática Aranzadi*, nº 23, pp. 1-10.
- MARTÍN-CASALLO LÓPEZ, J. (1996), Implicaciones de la Directiva sobre protección de datos en la normativa española, *Actualidad Informática Aranzadi*, nº 20, pp. 1-7.
- MUÑOZ GUTIÉRREZ, G. (1996), Problemática que ha suscitado la Instrucción I de la Agencia de Protección de Datos, *Actualidad Informática Aranzadi*, nº 18, pp. 11-14.
- QUÍLEZ ÁGREDA, E. y CEBRIÁN DEL MORAL, A. (1993), Sobre la inconstitucionalidad de la Ley de Protección de Datos Informáticos, *Actualidad Jurídica Aranzadi*, nº 8, pp. 6-7.
- PANIAGUA ZURERA, M. (1992), *Movimiento consumerista y movimiento cooperativo*, Ed. I.N.C., Madrid.
- PÉREZ LUÑO, A.-E. (1996), *Manual de informática y derecho*, Ed. Ariel, Barcelona.
- SEMPERE RODRÍGUEZ, C. (1984), Comentario al artículo 18 CE, AA. VV. coord. por Alzaga Villaamil, *Comentarios a la Constitución y a las Leyes políticas*, Tomo II, Ed. Edersa, Madrid, pp. 425-465.
- SERRANO ALBERCA, J. M. (1985), Comentario al artículo 18 CE, AA. VV. dir. por Garrido Falla, *Comentarios a la Constitución*, 2ª ed., Ed. Civitas, Madrid, pp. 377-381.
- VELÁZQUEZ BAUTISTA, R. (1993), *Protección jurídica de datos personales automatizados*, Ed. Colex, Madrid.