
El régimen jurídico del tratamiento autorizado de los datos de carácter personal en España

Francisco Fernández Segado*

1. Derecho a la intimidad, libertad informática y “Hábeas Data”

La irrupción de la información en el mundo del Derecho ha desencadenado un conjunto de nuevos problemas que han exigido la búsqueda de respuestas jurídicas adecuadas a la solución de aquéllos. El manejo de peligros antes inexistentes frente a ciertos derechos, como es el caso, muy especialmente, del derecho a la intimidad.

No es inoportuno recordar que el mismo concepto del derecho a la intimidad fue tributario en el momento de su nacimiento de un conjunto de nuevas circunstancias sociales que indujeron a Warren y Brandeis¹ a escribir su conocido trabajo publicado a fines de 1890. En efecto, a fines del pasado siglo, el poder de los medios de comunicación, y muy significadamente de la prensa, había crecido de tal forma que amenazaba flagrantemente con generar graves lesiones en la vida privada de las personas.

Las reflexiones de los citados autores son, por sí solas, bien significativas:

“Que el individuo deba recibir plena protección de su persona y de su propiedad es un principio tan viejo como el propio *common law*. No obstante, ha sido necesario de vez en cuando

* Catedrático de Derecho Constitucional Universidad de Santiago de Compostela.

1 “*The right to privacy*”, en *Harvard Law Review*, 4 1890-1891, pp.193 y sgtes.

redefinir la naturaleza exacta y la extensión de esa protección. Los cambios políticos, sociales y económicos entrañan el reconocimiento de nuevos derechos y el *common law* con su eterna juventud, crece para satisfacer las demandas de la sociedad”².

Tras reflexionar acerca de como el derecho a vivir significa el derecho a disfrutar de la vida, “el derecho a que nos dejen en paz” (*the right to be let alone*), Warren y Brandeis ponían de relieve el hecho de que recientes inventos y métodos comerciales hacían conveniente dar nuevos pasos en orden a asegurar el respeto a aquel derecho:

“Fotografías instantáneas y empresas periodísticas han invadido los recintos sagrados de la vida privada y doméstica y numerosos ingenios mecánicos amenazan con hacer buena la predicción según la cual lo que se susurra en el gabinete será proclamado desde los tejados”³.

Ante este estado de cosas, ante estas nuevas realidades sociales, los referidos autores se esforzarán en la búsqueda, a partir del *common law*, de los instrumentos necesarios con vistas a combatir las intromisiones ilegítimas en la vida privada⁴.

No es radicalmente nuevo, en consecuencia, el hecho de que el avance tecnológico haya vuelto a incidir sobre el derecho a la intimidad. La computación y el mundo de la inteligencia artificial a que ha dado lugar, ha posibilitado la acumulación ilimitada de informaciones que pueden ser memorizadas y transmitidas, permitiendo de esta guisa, como bien dice Frosini⁵, la aparición de un nuevo poder de dominio social sobre el individuo: el poder informático.

El profundo impacto de este nuevo poder social sobre ese derecho surgido en el marco del puritanismo de la sociedad bostoniana de fines del pasado siglo, furibundamente individualista, iba a desencadenar un

2 S. D. Warren y L. D. Brandeis: “*The right to privacy*”, *op. cit.*, p.193.

3 *Ibidem*, p. 195.

4 Acerca del reconocimiento jurisprudencial del derecho, cfr. F. Rigaux: “*L’élaboration d’un right to privacy par la jurisprudence ammericaine*”, en *Revue Internationale de Droit Comparé*, vol. XXXIII, 1980, pp. 701 y sgtes.

5 Vittorio Frosini: *Informática y Derecho*, Editorial Temis, Bogotá, p. 109.

no menos notable cambio de perspectiva en la concepción tradicional del *right to privacy*.

En efecto, al poder social informático, como nuevamente advierte Frosini⁶, se ha contrapuesto la “libertad informática”. Esta ya no es el antiguo *right to privacy* como derecho a la intimidad entendido como separación y defensa del individuo frente a la sociedad; es un nuevo derecho social de libertad; no es ya únicamente el derecho a negar la información sobre sí mismo, sino también el derecho a pretenderla. La libertad informática se nos perfila así como el derecho de disponer de la información, de preservar la propia identidad informática, o lo que es igual, de consentir, controlar y, en su caso, rectificar los datos informativos concernientes a la propia personalidad.

En suma, el *right to privacy* ha asumido una nueva dimensión por virtud de la cual ya no se entiende tan sólo en un sentido puramente negativo, de rechazo de la información de extraños en la vida privada, o de la transmisión de informaciones a ella referidas, en la más pura línea de los llamados derechos de la primera generación; bien al contrario, ha pasado a tener un contenido positivo por mor del cual se reconoce a cada persona el ejercicio de un control sobre el uso que pueda hacerse de los propios datos personales recogidos en un archivo electrónico de un centro de proceso de datos. La libertad informática encierra así un derecho de autotutela de la propia identidad informática, cuya primera exigencia es la protección de los datos informáticos personales frente a aquellas personas no autorizadas para conocerlos, procesarlos, modificarlos o difundirlos, razón por la que, como una vez más señala Frosini⁷, el primero de los contenidos cuya normación viene exigida por la efectividad de la nueva libertad es el del acceso al banco de datos, con el fin de, por un lado, poder disponer de toda la información almacenada en un archivo electrónico sobre la propia personalidad y, por otro, poder rectificar ciertos datos concernientes a la misma⁸. Nace así el Hábeas Data.

6 *Ibidem*, p. 35.

7 *Ibidem*, pp. 73-74.

8 En Italia, Enzo Roppo ha englobado dentro del contenido de la libertad informática estos cuatro derechos: a) el derecho de conocer si un determinado banco de datos contiene o no informaciones propias; b) el derecho de acceso, caso positivo, al contenido de aquellas informaciones; c) el derecho de rectificación, esto es, de poder corregir los datos imprecisos; y, d) el derecho de conocer qué información sobre la persona interesada fue comunicada a ter-

2. La protección de los datos personales frente a la utilización de la informática en el Derecho comparado

Las innovaciones experimentadas por el derecho a la intimidad han tenido su traducción inmediata tanto en la legislación como en la jurisprudencia de gran número de países.

Suelen considerarse como pioneras en este ámbito la Ley del *Land* de Hesse de 7 de octubre de 1970, reguladora de las bases de datos de su Administración, norma que creaba la figura del *Datenschutzbeauftragter*, esto es, del Comisario para la protección de la información, y la ley sueca de 11 de mayo de 1973 sobre protección de datos.

Con todo, por razones fácilmente comprensibles, es en Estados Unidos donde en mayor medida se ha profundizado en la problemática que nos ocupa. A partir de la promulgación, en 1966, de la *Freedom of Information Act*, los poderes públicos convirtieron en transparente para toda la comunidad datos e informaciones mantenidas en absoluto sigilo desde tiempo inmemorial. La *Fair Credit Reporting Act* de 26 de octubre de 1970, al acoger un conjunto de previsiones respecto a la recogida y transmisión de datos sobre la solvencia de las personas y los derechos que a los afectados reconoce para su protección, inaugura, como se ha advertido⁹, una técnica que luego se aplicará preferentemente a la tutela de las informaciones personales recogidas y tratadas mediante computadoras.

El 31 de diciembre de 1974 la *Privacy Act* incorporará a su articulado buena parte de las recomendaciones propuestas un año antes por el Departamento de Salud, Educación y Bienestar (en su estudio sobre "Registros, computadoras y derechos de los ciudadanos", en el que se proponía la elaboración de un código federal de *fair information practices* encaminado a salvaguardar la intimidad personal). Las líneas maestras de la referida Ley de 1974 eran las siguientes: a) restringida la utilización de la información que sobre los individuos disponga el gobierno federal, requiriendo a las agencias públicas la creación de un registro

ceros y con qué finalidad. Enzo Roppo: "Informática, tutela della privacy e diritti della libertà", en el colectivo, *Computers e responsabilità civile*, Giuffrè, Milano, 1985, pp. 28-29.

9 Pablo Lucas Murillo: "La protección de los datos personales ante el uso de la informática", en *Revista de la Facultad de Derecho de la Universidad Complutense de Madrid*, núm. 15 (monográfico), pp. 601 y sgtes. especialmente p. 607.

donde se hiciera constar la información suministrada; b) establecía restricciones a la recogida y conservación de información personal, obligando al gobierno a obtenerla directamente del interesado cuando ello fuera posible, a comunicarle el uso que se hiciera de esa información y a conservar tan sólo aquella que fuere pertinente y necesaria para el cumplimiento de los fines de la agencia, y c) reconocía el derecho de acceso a los propios datos y a obtener copia de ellos, así como a exigir su rectificación, pudiendo recabar el afectado la revisión judicial de las resoluciones negativas que al respecto dictara la Administración.

En 1977, la *Privacy Protection Study Commission*, contemplada por la Ley de 1974, hizo públicas las conclusiones de las investigaciones desarrolladas, cuyos propósitos básicos consistían en: reducir al máximo la intrusión gubernamental en las vidas de la gente; maximizar la observancia de las reglas de corrección, y crear de esta forma una legítima expectativa de intimidad y confidencialidad sobre la información personal.

Los parámetros básicos del régimen jurídico de la informática, en lo que toca a la intimidad informativa, quedaban de esta forma recogidos en las normas expuestas y en los principios citados, si bien el panorama legislativo en Estados Unidos bien puede completarse con un largo rosario de normas legales que se refieren a aspectos puntuales.¹⁰

Bien puede decirse, en resumen, que entre 1974 y 1986 un conjunto de normas legales ha posibilitado el ordenamiento jurídico de aspectos diversos en relación a la materia que nos ocupa, y entre ellos: a) la revelación de informaciones (*disclosure of the information*); b) la ordenación del procedimiento a seguir para el ejercicio de los derechos de acceso (*right of acces*), rectificación (*correction*), o complemento (*amendment*) de los registros informáticos, y c) el procedimiento judicial necesario para conferir plena efectividad a los anteriores derechos.

En la República Federal Alemana, el Parlamento Federal aprobaba en 1977 la *Datenschutzgesetz*, ley federal de protección de datos, disciplinando el almacenamiento en registros informáticos de datos, tanto por las autoridades federales como por entidades privadas. En un importante fallo -la Sentencia de 15 de diciembre de 1983- el Tribunal Constitucional Federal, interpretando la ordenación normativa inme-

10 Cfr. al efecto, Pablo Lucas Murillo: "La protección de los datos personales...", *op. cit.*p. 608.

diatamente anterior, entendía que sólo podía considerarse admisible, desde la óptica constitucional, la recogida y ulterior almacenamiento de informaciones referidas a “sucesos íntimos” (*intime Vorgänge*) cuando se conozca la finalidad para la que vayan a ser utilizadas. Se ha podido hablar de esta forma en Alemania de un derecho a la autodeterminación informativa o de las informaciones (*informationelle Selbstbestimmungsrecht*), concepto que ha hecho suyo un sector de la doctrina española¹¹.

En Inglaterra, a partir del conocido como “Informe Younger sobre la intimidad”, publicado en julio de 1972, y del Informe presentado en 1978 por el *Data Protection Committee*, se iban a fijar las bases que juridificarían las normas legales sobre la materia, básicamente, la *Data Protection Act* de 1984. La ley se esfuerza por hacer transparente la recogida y circulación de los datos de carácter personal con el fin de soslayar todo posible abuso. Como bien recuerda Lucas Murillo¹², este espíritu se contiene en los ocho principios que pretenden condensar el significado de la Ley británica y que ésta misma enuncia con el objeto de facilitar la tarea del intérprete, principios de los que nos hacemos eco a continuación:

- I. Los datos personales han de recogerse y procesarse con lealtad y legalmente.
- II. Los propósitos para los que se recogen datos personales deben ser legales y han de especificarse.
- III. El uso y revelación de datos personales deben ser compatibles con los propósitos para los que se conservan los datos.
- IV. La calidad y extensión de los datos personales deben ser adecuadas, pertinentes y no desproporcionadas respecto a los propósitos para los que se conservan.
- V. Los datos personales han de ser precisos y deben actualizarse cuando sea necesario.
- VI. No se pueden conservar los datos personales más tiempo que el estrictamente necesario para la consecución del propósito perseguido.

11 Pablo Lucas Murillo: *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

12 *Ibidem*, p.609.

- VII. Toda persona tiene derecho: a) a intervalos razonables y sin retrasos ni gastos injustificados: a ser informada por quien maneje datos de si conserva datos suyos, y a acceder a tales datos, y b) cuando sea preciso, a corregir o cancelar dichos datos.
- VIII. Es preciso adoptar medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado, su alteración, revelación o destrucción o su pérdida accidental.

El propio Tribunal Europeo de Derechos Humanos, en su Sentencia de 6 de setiembre de 1978 (Caso Klass y otros), en la que se pronunciaría sobre la compatibilidad de ciertos preceptos de la Ley alemana de 13 de agosto de 1968, que restringe en ciertos supuestos el secreto de la correspondencia y de las comunicaciones telegráficas y telefónicas, con el Art.8º del Convenio de Roma (que reconoce el derecho de toda persona al respecto de su vida privada), afirmarí literalmente: "Característico del Estado-policía, el poder de vigilar en secreto a los ciudadanos no es tolerable según el Convenio como medida estrictamente necesaria en la salvaguarda de las instituciones democráticas".¹³

Los más recientes textos constitucionales han llegado incluso a incorporar a su articulado el contenido de la libertad informática. Es el caso de la Constitución de Portugal, cuyo Art. 35.1, tras la redacción dada al mismo en la reforma de 1982, prescribe que: "*Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos informáticos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização*". Más aún, en la misma reforma de 1982, uno de los nuevos párrafos adicionados al Art. 35º (el actual apartado segundo) prohíbe no sólo el acceso de terceros a ficheros con datos personales, sino también la respectiva interconexión, lo que se ha justificado¹⁴ en la circunstancia de que el más grave problema que para la libertad encierra la informática es el de que el proceso automático de datos facilita la interconexión de ficheros, permitiendo de esta forma la creación de grandes bancos de datos en los que se

13 Puede verse esta Sentencia en el **Boletín de Jurisprudencia Constitucional**, núm. 30, octubre 1983, pp.1199 y sgtes. Especialmente, p. 1208 (Consideraciones de Derecho, II, epígrafe 42).

14 José Antonio Barreiros: "*Informática, liberdades e privacidade*", en el colectivo, *Estudos sobre a Constituição*, vol. I, Lisboa, 1977, p. 132.

plasma una suerte de retrato total del sujeto a que se refieren, y tal retrato puede ser en muchas ocasiones enormemente deformador.

En definitiva, frente a la informática se tutela la intimidad o, si así se prefiere, la autodeterminación informativa, descansando la técnica que a este fin se utiliza (la protección de datos) tanto en la prohibición de recoger de forma individualizada los datos que se consideran individualísimos (también llamados “datos sensibles”), como en el sometimiento de la recogida, elaboración, almacenamiento y transmisión de los restantes y rígidas limitaciones encaminadas a asegurar su veracidad y proporcionalidad, así como en el control de los interesados sobre la información que les afecta, lo que se consigue no sólo garantizando su acceso a los datos que les atañen, sino también su derecho a rectificarlos o cancelarlos.

3. El Convenio Europeo de 28 de Enero de 1981

El 28 de enero de 1981, en Estrasburgo, se firmaba el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, por los estados miembros del Consejo de Europa, que buscaban a través del mismo la ampliación de la protección del derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados, con vistas, en último término, a la conciliación de los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.

El Convenio tiene como finalidad garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueran su nacionalidad o su residencia el respeto, en general, de sus derechos y libertades fundamentales y, en particular, de su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona, entendiéndose, a los efectos del Convenio, por “datos de carácter personal”, cualquier información relativa a una persona física identificada o identificable (persona concernida), y por “tratamiento automatizado”, las operaciones de registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión, operaciones todas ellas efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados.

El ámbito de aplicación del Convenio atañe a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado. Aunque el Convenio posibilita a un Estado parte la inaplicabilidad del mismo a determinadas categorías de ficheros automáticos de datos de carácter personal, impide al unísono que puedan ser excluidos de la aplicación del Convenio ficheros automatizados sometidos, con arreglo al derecho interno del Estado de que se trate, a disposiciones de protección de datos. De igual forma, se posibilita la aplicación del Convenio a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica, como también a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.

El Convenio, a la par que establece un conjunto de previsiones en orden a garantizar la calidad de los datos y prevé la adopción de medidas de seguridad apropiadas para la seguridad de los mismos, se refiere específicamente a unas categorías particulares de datos, los que podríamos denominar “datos sensibles”: los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, categorías todas ellas que no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas, regla que se prevé que haya de regir asimismo en el caso de datos de carácter personal referentes a condenas penales.

Las determinaciones del Convenio orientadas a garantizar la calidad de los datos de carácter personal objeto de un tratamiento automatizado son estas:

- a. Los datos en cuestión se han de obtener y tratar leal y legítimamente.
- b. Se han de registrar para finalidades determinadas y legítimas, no pudiendo utilizarse de forma incompatible con dichas finalidades.
- c. Serán (dichos datos) adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.
- d. Serán exactos y si fuera necesario puestos al día.
- e. Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Con vistas a la seguridad de los datos de carácter personal registrados en ficheros automáticos, el Convenio prevé la adopción de medidas de seguridad adecuadas para su protección contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

A modo de garantías complementarias para la persona concernida, el Art. 8º del Convenio reconoce a cualquier persona los siguientes derechos:

- a. El derecho a conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.
- b. El derecho a obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal concernientes a dicha persona, así como la comunicación de dichos datos en forma inteligible.
- c. El derecho a obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados por el Convenio en relación a la calidad de los datos y a los “datos sensibles”.
- d. El derecho, finalmente, a disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de rectificación o de borrado.

El Convenio no admite excepción alguna en las disposiciones relativas a la calidad de los datos, a los “datos sensibles” y a los derechos reconocidos respecto de una persona concernida por un fichero automatizado de datos, con la única y exclusiva salvedad de que tal excepción, prevista por la ley del Estado parte, constituya una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales, como también para la protección de la persona concernida y de los derechos y libertades de otras personas. Por lo demás, el Convenio permite que la ley pueda prever restricciones en el ejercicio de los derechos a obtener comunicación sobre la existencia en un fichero de datos de carácter personal, a

la rectificación o borrado de dichos datos y a la disposición de un recurso, en relación con los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Finalmente, de conformidad con el Art. 10º del Convenio, cada parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos que enuncia el mismo Convenio.

4. La constitucionalización en España de la protección de los datos personales frente al uso de la informática.

El Art. 18.4 de la Constitución Española, en buena medida siguiendo de cerca el modelo portugués, iba a contemplar la conveniencia de limitar el uso de la informática con vistas a garantizar los derechos de los ciudadanos. A tenor del citado precepto:

“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”.

Esta previsión apareció ya en el mismo texto del Anteproyecto, siendo tan sólo objeto de una reforma significativa en la Comisión de Asuntos Constitucionales y Libertades Públicas del Congreso de los Diputados con ocasión, especialmente, de la discusión de dos enmiendas, una del diputado del Grupo Parlamentario de UCD, señor Sancho Rof, y otra, del diputado del Grupo de la Minoría Catalana, señor Roca i Junyent. Estas dos enmiendas, de objetivos contrapuestos, ofrecieron la ocasión, como bien advierte Lucas Murillo, para reiterar la importancia de la cuestión y enfatizar la necesidad de adoptar medidas legislativas de protección.¹⁵

¹⁵ Pablo Lucas Murillo: “El derecho a la autodeterminación informativa”, *op. cit.*, p. 151.

Mientras el Sr. Sancho Rof abogó en su enmienda por la supresión del precepto transcrito, al entender que nada añadía al reconocimiento general del Art. 18.7 CE (Constitución Española), garantizando el derecho al honor, a la intimidad personal y familiar y a la propia imagen, entrañando, por el contrario, el riesgo de quedar obsoleto frente a la aparición de nuevos avances tecnológicos que amenazaren los citados derechos, posicionamiento que no prosperaría, el Sr. Roca i Junyent vino a proponer la ampliación del ámbito material que con la ley a la que se remite el Art. 18.4 CE se pretende proteger, que en un primer momento se circunscribía a los derechos personalísimos del Art. 18.1 CE.

A juicio del diputado catalán¹⁶, cuando la Ponencia limita el uso de la informática a los daños que puedan producirse al honor y a la intimidad personal y familiar, se queda simplemente en una reflexión parcial de los problemas, “porque 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 incluso ni 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 ciudadanos”.

La Comisión aceptaría el planteamiento precedentemente expuesto, con lo que ello entrañaba de reconocimiento por parte del constituyente de la sustancial diferencia existente entre el ámbito de la intimidad personal y familiar y del honor y el propio de la protección de datos.

La determinación del Art. 18.4 ha de complementarse necesariamente con la del Art. 105º, b) CE, a tenor del cual: “La ley regulará: b) el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas”. Para redondear lo que Pérez Luño denomina el “círculo hermético”¹⁷ hay que referirse

16 Diario de Sesiones del Congreso de los Diputados, Comisión de Asuntos Constitucionales y Libertades Públicas, núm. 70, 19 de mayo de 1978, p. 2527.

17 Antonio Enrique Pérez Luño: *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1984, p. 341.

también a la previsión del Art. 20.4 CE, de conformidad con el cual: “Estas libertades (las libertades informativas, de cátedra y de producción y creación literaria, artística, científica y técnica) tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollan y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia”.

Una cuestión de interés que se puede suscitar al hilo del Art. 18.4 CE es la de si cabe ver en el mismo el reconocimiento de un derecho fundamental o si, por el contrario, se trata de un mero mecanismo de garantía.

Es evidente, a la vista de la propia dicción del Art. 18.4 CE, que este precepto no sólo pretende proteger la intimidad y el honor, sino también el pleno ejercicio de los derechos ciudadanos. Se trata, en consecuencia, de limitar el uso de la informática por cuanto el constituyente estima que del mismo pueden derivarse amenazas para el conjunto de derechos ciudadanos. El conjunto de componentes normativos del Art. 18º CE tiene como punto de referencia a la persona y a aquellas manifestaciones de la misma que le son más propias. Por tanto, como indica Lucas Murillo¹⁸, no parece descabellado identificar en la defensa de la personalidad -como clave genérica- el bien a proteger. De esta forma, dicho bien jurídico objeto de protección desborda a la intimidad, propiciando la configuración de un nuevo derecho fundamental.

En esta misma dirección, el Juez de la Constitución¹⁹, tras estimar que el Art. 18.4 CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva modalidad de amenaza concreta a la dignidad y a los derechos de la persona, entiende que 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, lo que la Constitución llama “la informática”.

18 Pablo Lucas Murillo: “La protección de los datos personales ante el uso de la informática”, *op. cit.*, p. 614.

19 Sentencia del Tribunal Constitucional (en adelante STC) 254/1993, de 20 de julio, fundamento jurídico 6º.

5. El contenido mínimo del derecho a la libertad frente a las agresiones provenientes de un uso ilegítimo de la informática.

El Art. 18.4 CE se remite a la ley a los efectos de regular normativamente ese instituto que a la par es garantía de un conjunto de derechos, pero también, en sí mismo, un derecho o libertad fundamental. Y esa ley de desarrollo constitucional es la Ley Orgánica 5/1992, del 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Es decir, transcurrieron catorce años desde la entrada en vigor de la Constitución hasta la aprobación de la citada Ley Orgánica (LORTAD).

En el transcurso de ese período, España ratificaba por Instrumento del 27 de enero de 1984, el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, al que ya nos referimos.

Con anterioridad a la aprobación de la LORTAD, se interponía ante el Tribunal Constitucional el recurso de amparo núm. 1.827/1990, contra la degeneración presunta, por parte del Gobernador Civil de la provincia de Guipúzcoa y del Ministro del Interior, de la comunicación de la información que había solicitado el actor acerca de sus datos de carácter personal que obraban en ficheros automatizados de la Administración del Estado, así como contra la Sentencia de la Audiencia Territorial (Sala de lo Contencioso-Administrativo) de Pamplona de 1989, y la dictada por el Tribunal Supremo (Sala Tercera, Sección octava) del 30 de abril de 1990, que confirmaron la presunta denegación administrativa por entender que el Convenio Europeo de 1981 (en el que se fundaban las peticiones de información) no era de aplicación directa, siendo preciso el complemento de la actividad legislativa y reglamentaria interna para la aplicación práctica de sus disposiciones en España.

El Tribunal Constitucional iba a entender, en línea con una jurisprudencia muy reiterada desde la Sentencia 38/1981, que los textos internacionales ratificados por España despliegan ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución.

A partir de la consideración, ya expuesta anteriormente, de que el Art. 18.4 CE diseña, a la vez que un instituto de garantía, un auténtico

derecho a la libertad frente a las potenciales agresiones a la libertad de la persona provenientes de un uso ilegítimo de la informática, el Alto Tribunal constata que el primer problema que el derecho en cuestión suscita es el de la ausencia, hasta un momento posterior a los hechos que dan lugar a la demanda, de un desarrollo legislativo del mismo. Ahora bien, aun en la hipótesis de que un derecho constitucional requiriese de la *interpositio legislatoris* para su desarrollo y plena eficacia, la jurisprudencia constitucional ha negado que el reconocimiento constitucional de un derecho no tenga otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar *per se* pretensiones individuales, de modo que sólo sea exigible cuando el legislador lo haya desarrollado.

Cuando se opera con una “reserva de configuración legal” es posible -razona el Alto Tribunal²⁰ - que el mandato constitucional no tenga, hasta que la regulación se produzca, más que un mínimo contenido. A partir de aquí se plantea lógicamente el problema del cuál deba ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo.

Un primer elemento, el más “elemental”, de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria.

Si se nos permite el *ex cursus* acerca del ámbito, significación y función de los derechos fundamentales en el constitucionalismo de nuestro tiempo inspirado en el Estado social de Derecho, cabe significar que la doctrina ha puesto de manifiesto -en coherencia con los contenidos y estructuras de los ordenamientos positivos- que los derechos fundamentales no incluyen solamente derechos subjetivos de defensa de los individuos frente al Estado, y garantías institucionales, sino también deberes positivos por parte de éste²¹.

20 STC 254/1993, de 20 de julio, fund. jur. 6º, *in fine*.

21 En el mismo sentido se ha pronunciado el Alto Tribunal. STC 53/1985, de 11 de abril, fund. jur. 4º.

En sintonía con la precedente reflexión, el Juez de los derechos fundamentales ha entendido²² que la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada “libertad informática” es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (hábeas data).

El incremento de medios técnicos de tratamiento de la información puede propiciar un uso desviado de ésta y, consecuentemente, la efectiva invasión de la esfera privada de los ciudadanos afectados. Correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se hayan de otorgar al ciudadano, para salvaguardar el núcleo esencial de su derecho.

Como señala el Tribunal²³, la constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de la Administración donde obran datos personales de un ciudadano son absolutamente necesarios para que los intereses protegidos por el Art. 18º CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos.

Y en otro momento²⁴, el “intérprete supremo de la Constitución”, como lo define el Art. 1.1 de su Ley Orgánica, ha convenido en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera que lo harían las intromisiones directas en el contenido nuclear de ésta.

22 STC 254/1993, de 20 de julio, fund. jur. 7º.

23 *Ibidem*.

24 STC 143/1994, de 9 de mayo, fund. jur. 7º.

Así se desprende, también, de los compromisos internacionales suscritos por España en la materia, y, en especial, del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por España, como ya señalamos, en cuanto impone a los Estados firmantes; principios específicos de actuación para la obtención de datos que garanticen la legitimidad de éstos y la adecuación de la información recibida en atención a las finalidades con ella perseguidas; un especial refuerzo de la reserva de datos en materias especialmente conectadas con el derecho a la intimidad, y la no difusión de “datos de carácter personal”.

En definitiva, si el derecho a la intimidad no agota su contenido en facultades puramente negativas, de exclusión, mucho menos aún lo hace el derecho a la libertad frente a las agresiones provenientes de un uso ilegítimo de la informática, que nos ofrece un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona, esto es, un derecho a controlar el uso de los mismos datos insertos en un programa informático.

6. El desarrollo legislativo del artículo 18.4 CE

Como ya hemos tenido oportunidad de recordar, la ley a que se refiere el Art. 18.4 CE iba a tardar casi tres lustros en ser aprobada. Ello no obstante, de modo fragmentario y parcial, diferentes disposiciones legislativas y reglamentarias suministraban una protección del derecho recogido por el referido precepto constitucional.

Así, 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, en su disposición transitoria primera, determinaba que: “En tanto no se promulgue la normativa prevista en el artículo 18º, apartado 4, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley”.

Bien es verdad que, como señalara Lucas Murillo²⁵, esta solución

25 Pablo Lucas Murillo: “El derecho a la auto determinación informativa”, *op. cit.*, pp. 159-160.

era claramente insuficiente, y ello por cuanto los daños que una persona puede sufrir como consecuencia de la elaboración informática de los datos relativos a ella misma no provendrán normalmente tanto de las informaciones reservadas que puedan sufrir ese destino, cuanto de la recogida y tratamiento de aquellas referencias personales de apariencia, en principio, inofensiva, o no reservada. Por eso, si se tiene en cuenta que todo el sistema defensivo de la Ley Orgánica N° 1/1982 descansa en el concepto de intromisión ilegítima y que ésta se concibe como una invasión subrepticia en la vida personal íntima se comprenderá con facilidad la razón por la que este régimen transitorio no podía dar demasiado juego en el ámbito que nos ocupa.

También era de aplicación, como ya se ha puesto de relieve, el Convenio europeo de 1981, si bien es preciso recordar que el Art. 4.1 del mismo preveía que: "Cada parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo". Ello significa que el Convenio se remite a los ordenamientos internos, que son los que han de precisar el específico sistema de garantías.

Al margen ya de las normas citadas, en otras leyes estatales encontramos previsiones que pueden ser de interés en relación con la materia que nos ocupa. Es el caso de la Ley General Tributaria, cuyo Art. 111.1 (tras su reforma acaecida en 1985) prevé de modo específico que el deber de colaboración con la Hacienda Pública facilitando los datos de relevancia a los efectos tributarios no alcanza a los datos privados no patrimoniales cuya revelación pudiera suponer un atentado contra el honor, la intimidad personal o familiar o la propia imagen.

También en el campo tributario tiene especial interés el Art. 1° de la Orden del Ministerio de Hacienda de 30 de julio de 1982, a cuyo tenor, toda la información contenida en las bases de datos de la Hacienda Pública, con independencia de que sea personal, económica o estrictamente fiscal o de que afecte a personas físicas o jurídicas, será de uso exclusivamente reservado para el cumplimiento de los fines que el ordenamiento jurídico encomienda al Ministerio de Hacienda.

La Ley Orgánica N° 5/1985, del Régimen Electoral General, prohíbe en su Art. 41.2, en relación con el censo electoral, toda información particularizada sobre datos personales que obren en él, con algunas excepciones muy puntuales, como, por ejemplo, las informaciones de esa naturaleza que se soliciten por vía judicial.

En análoga dirección, alguna disposición de la Ley General de Sanidad insiste, frente a las administraciones sanitarias, en la ineludibilidad de respetar el derecho de todo ciudadano a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público.

Recordemos finalmente que la Ley N° 12/1989, de la Función Estadística Pública, establece específicamente el secreto estadístico para la protección de los datos personales obtenidos por los servicios estadísticos tanto de los informantes, cuanto de las administraciones públicas.

Este conjunto de normas era, con todo, insuficiente en orden al necesario desarrollo constitucionalmente exigido por el Art. 18.4 CE. Y no dejaba de ser anómalo el excesivo tiempo transcurrido para el adecuado cumplimiento del mandato del citado precepto constitucional.

Quizá las exigencias impuestas por el Acuerdo de Schengen fueran decisivas en orden a este desarrollo legislativo²⁶. En efecto, el 25 de junio de 1991, el Plenipotenciario de España firmaba en Bonn el Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los gobiernos de los estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes. Recordemos que el Título VI del referido Acuerdo contemplaba la “protección de los datos de carácter personal” (artículos 126° a 130°), y que el Acuerdo de Adhesión del Reino de España al citado Convenio contiene una declaración común de las partes contratantes por cuya virtud “el Gobierno del Reino de España se obliga a adoptar, antes de la ratificación del Acuerdo de Adhesión al Convenio de 1990 (el Convenio de Schengen), todas las iniciativas necesarias para que la legislación española sea completada de conformidad con el Convenio europeo de 28 de enero de 1981 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal y con observancia de la Recomendación R (87) 15, de 17 de septiembre de 1987, del Comité de Ministros del

26 Carlos Ruiz Miguel: “En torno a la protección de los datos personales automatizados”, en *Revista de Estudios Políticos*, núm. 84, abril-junio 1994, pp. 237 y sgtes.; especialmente, p. 237.

Consejo de Europa, tendente a reglamentar la utilización de los datos de carácter personal en el sector policial”.

Junto al Título anteriormente referido del Acuerdo de Schengen, si se nos permite el *ex cursus*, el Convenio de aplicación del Acuerdo dedica otro de sus títulos (el cuarto) al “sistema de información de Schengen”. Dentro de ese título, su Capítulo tercero regula la protección de los datos de carácter personal y la seguridad de los datos en el marco del sistema de información de Schengen. Los artículos 109º, 110º y 111º reconocen a toda persona un conjunto de derechos, entre ellos: el derecho de acceso a los datos que se refieran a ella y estén introducidos en el sistema de información de Schengen; el derecho de rectificación de aquellos datos que contengan errores de hecho o de supresión de los datos que contengan errores de derecho referidos siempre a la persona en cuestión, y el derecho a emprender acciones, en el territorio de cada parte contratante, ante el órgano jurisdiccional o la autoridad competente en virtud del Derecho nacional, en particular a efectos de rectificación, supresión, información o indemnización motivadas por una descripción que se refiera a ella.

El Convenio de aplicación del Acuerdo establece (artículos 112º y 113º) asimismo la necesidad de que los datos de carácter personal introducidos en el “sistema de información de Schengen” a efectos de la búsqueda de personas se conserven tan sólo durante el tiempo necesario para los fines para los que se hubieren facilitado dichos datos. En cualquier caso, tres años después de su introducción como máximo, la parte contratante informadora deberá examinar la conveniencia de conservarlos. Ese plazo se reduce a un año respecto a ciertos datos (los contemplados por el Art. 99º) y se amplía a diez años en el supuesto de datos que no tengan carácter personal.

Digamos por último que el Art. 114º del Convenio contempla una suerte de garantía institucional, al obligar a cada parte contratante a designar una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre el fichero de la parte nacional del “sistema de información de Schengen”, así como de comprobar que el tratamiento y la utilización de los datos introducidos en el “sistema de información” no atentan contra los derechos de la persona de que se trate. Al unísono, el mismo precepto reconoce a toda persona el derecho a solicitar a las autoridades de control que comprueben los datos referentes a ella integrados en el “sistema de información”, como también el uso que se haga de dichos datos.

Como antes señalamos, es posible que el Acuerdo de Schengen fuera el detonante que desencadenara la reacción del legislador español, que, a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), procedía a desarrollar el Art. 18.4 CE, ordenando normativamente esta materia.

7. Rasgos generales de la ordenación jurídica del tratamiento automatizado de datos de carácter personal.

La LORTAD tiene como ámbito de aplicación los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado, así como toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado. Este ámbito de aplicación se perfila por exclusión, complementariamente, al quedar fuera del mismo, entre otros, los datos anónimos, los que constituyan información de dominio público o aquellos otros que recojan información con la finalidad, precisamente, de darla a conocer al público en general (como pueden ser los registros de la propiedad o mercantiles).

La LORTAD deja vigentes las regulaciones especiales que contienen, por lo general, suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico. Tal acontece con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así sucede asimismo con los ficheros regulados por la Ley 12/1989, de 12 de mayo, sobre función estadística pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. Quedan de igual manera fuera del ámbito de la ley aquellos datos que, en virtud de intereses públicos prevalentes, no deben estar sometidos a su régimen cautelar (este es el caso de los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el Art. 68º de la Ley 17/1989, de 19 de julio, reguladora del régimen del Personal Militar Profesional).

El bien jurídico que la ley pretende garantizar es justamente el conjunto de derechos a los que alude el Art. 18.4 CE, esto es, el derecho

al honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. En todo caso, con esta previsión, que acoge su Art. 1º, la LORTAD no aclara la polémica suscitada al respecto, esto es, la de si ese bien es la intimidad o, por contra, se desborda la intimidad para proteger ese derecho que el Tribunal Constitucional Federal alemán denominara “derecho a la autodeterminación informativa”. Recordemos que, a juicio del citado Tribunal²⁷, del Art. 2.2 de la Ley Fundamental de Bonn (“Cada uno tendrá derecho a la vida y a la integridad física y será inviolable la libertad de la persona. Estos derechos sólo podrán verse afectados en virtud de una ley”) dimana “la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida”.

Entre nosotros, Lucas Murillo²⁸ ha diferenciado el derecho a la intimidad, un clásico derecho de defensa, según este autor, que casa mal con la técnica de la protección de datos, entre otras consideraciones, porque los datos que se protegen no tienen por qué ser íntimos, siendo suficiente con que se trate de datos personales, aunque sean inocuos, circunstancia que conduce al mismo autor²⁹ a propugnar el abandono de la referencia a la intimidad y la correlativa opción en favor de un nuevo derecho: el derecho a la autodeterminación informativa.

En todo caso, lo que resulta inequívoco en la LORTAD es que la amenaza potencial a la que se trata de hacer frente con la ley, desencadenada por el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos, recae sobre la privacidad. Como se precisa en la propia Exposición de Motivos de la LORTAD, se ha de notar que se habla de “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 las personas (el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos,

27 Sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983. *BverfGE*, 65, 1 y sgtes. La sentencia puede verse traducida por Mariano Daranas en el *Boletín de Jurisprudencia Constitucional*, nº 33 (1984), pp. 126 y sgtes.

28 Pablo Lucas Murillo: *Informática y protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1993, pp. 27 y sgtes.

29 *Ibidem*, pp. 32-33.

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. Queda claro, pues, que es la privacidad así entendida lo que trata de salvaguardarse por la LORTAD. La propia Exposición de Motivos de la norma legal concluye poniendo de relieve, en lo que ahora interesa, que mientras la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros apartados del Art. 18º CE y por las leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

En resumen, de modo genérico, bien puede decirse que la finalidad de la ley es hacer frente a los riesgos que para los derechos de la persona puede suponer el acopio y tratamiento de datos por medios informáticos.

Para dar una adecuada respuesta a las exigencias que dimanen del cumplimiento de esa finalidad, la ley se nuclea en torno a los que convencionalmente se denominan "ficheros de datos". La LORTAD introduce el concepto de "tratamiento de datos" ("operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"), concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar un determinado perfil personal.

La LORTAD está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. A tal efecto se estructura la ley en una parte general y otra especial. La primera -como se reconoce en la Exposición de Motivos- atiende a recoger los principios en los que ha cristalizado una *opinio iuris* generada a lo largo de dos décadas, definiendo derechos y garantías encaminados a asegurar la vigencia de tales principios. Los principios reguladores de la recogida, registro y

uso de datos personales y, sobre todo, las garantías de la persona, constituyen la médula ósea de esta primera parte de la ley.

En su parte especial, la LORTAD trata de articular los extremos concretos que han de regir los ficheros de datos, a cuyo efecto comienza distinguiendo entre los distintos tipos de ficheros, según sea su titularidad pública o privada. Otra disposición de la parte especial que ha de ser destacada es la atinente a la transmisión internacional de datos, aspecto en el que la ley traspone la norma del Art. 12º del Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos, solución que pretende conciliar la protección de la integridad de la información personal con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual (pensemos, por poner dos ejemplos concretos, en las transferencias bancarias y en las reservas de pasajes aéreos).

Una última observación ha de hacerse en relación con la norma legal que nos ocupa. Sobre su interpretación ha de incidir de modo inexcusable la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, que incide en distintos ámbitos del ordenamiento jurídico interno y, como bien se ha dicho³⁰, supone, ante todo, la necesidad de una nueva consideración de la Ley Orgánica Nº 5/1992, a la luz de sus principios y disposiciones. En todo caso, es preciso partir de la idea de que tanto esta última Ley Orgánica como la aludida Directiva tienen su origen común en el tantas veces citado Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981.

Es por ello mismo, por lo que la Ley Orgánica Nº 5/1992, LORTAD, atendió ya en su nacimiento conceptos fundamentales que aparecen en la mencionada Directiva 95/46/CE, que, por otra parte, no tienen un reflejo legal tan claro en el resto de los países de la Unión Europea. Este es el caso, por ejemplo, de dos de los pilares básicos del tratamien-

30 María José García Beato: "Principios y Derechos en la Ley Orgánica Nº 5/1992, de 29 de octubre, y en la Directiva 95/46/CE", en el colectivo, *Jornadas sobre el Derecho español de la protección de datos personales*, Agencia de Protección de Datos, Madrid, 1996, pp. 33 y sgtes.; especialmente, p. 35.

to automatizado de datos de carácter personal: de un lado, el principio del consentimiento del afectado, y de otro, el derecho de información del propio afectado.

8. Sujetos activos y pasivos

I. Aunque el Art. 18.4 CE parece limitar tan sólo a los ciudadanos la titularidad de estos derechos de personalidad, tal interpretación literal es inasumible. En cuanto estos derechos son inherentes a la propia dignidad del ser humano, parece incuestionable que de ellos deben gozar todas las personas, esto es, españoles y extranjeros.

Una interpretación sistemática de nuestra norma suprema conduce a esa solución por cuanto el Art. 13.1 CE establece que: “Los extranjeros gozarán en España de las libertades públicas que garantiza el presente Título en los términos que establezcan los tratados y la ley”. A partir de este precepto constitucional no debe extrañar que el legislador, en sede orgánica, haya, con carácter general, sentado el principio de que los extranjeros gozan en España de los mismos derechos que los españoles, como viene a establecer la Ley Orgánica N° 7/1985, de 1° de julio, sobre derechos y libertades de los extranjeros en España.

La LORTAD, en la misma dirección, habla ya en su Art. 1° de la necesidad de garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. Esto es, alude específicamente a las personas físicas en general y no a los ciudadanos. No podía ser de otro modo si se advierte que también el Art. 1° del tantas veces referido Convenio de 28 de enero de 1981, dispone que el fin del Convenio es garantizar en el territorio de cada parte, a cualquier persona física, sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, y en concreto, su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

Se ha cuestionado la doctrina de la titularidad por las personas jurídicas de estos derechos. Tanto Pérez Luño³¹ como Lucas Murillo³²,

31 Antonio Enrique Pérez Luño: “Los derechos humanos en la sociedad tecnológica”, en M. Losano y otros, *Libertad informática y leyes de protección de datos*, Centro de Estudios Constitucionales, Madrid, 1990, p. 154.

32 Pablo Lucas Murillo: “El derecho a la autodeterminación...”, *op. cit.*, pp. 181-182.

optan por admitir la titularidad por parte de las personas jurídicas de estos derechos. A juicio de este último, en cuanto que las personas jurídicas no son sino instrumentos de que se valen los hombres para alcanzar determinados fines que de otro modo serían de más difícil consecución, puede considerarse que hay argumentos de peso en pro del reconocimiento de aquella titularidad. Sin embargo, y al margen ya de cualquier opción doctrinal, lo cierto es que la LORTAD ha rechazado y excluye expresamente dicha titularidad, al aludir de modo específico en su Art. 1º, como ya indicamos, a las personas físicas, siguiendo de esta forma la pauta adoptada por algunos países (Alemania, Francia, Irlanda, etc.) y separándose de la establecida en otros que sí reconocen la titularidad de las personas jurídicas en este orden de derechos (Austria, Dinamarca, Islandia, etc.).

II. Sujeto pasivo es quienquiera que sea responsable de un fichero automatizado de datos de carácter personal, como asimismo todo aquél que decida sobre la finalidad, contenido y uso del tratamiento de esos datos. De igual forma, a la vista del Art. 10º LORTAD, han de ser considerados sujetos pasivos quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal. Como subraya Lucas Murillo³³, tratándose de datos personales, no importa la finalidad concreta para la que se haya creado un fichero o el objetivo específico que inspire su tratamiento, aunque, ciertamente, determinadas actuaciones (como las relativas a la salud o a la investigación científica) merecen un régimen parcialmente específico.

La LORTAD centra su atención en los poderes públicos, si bien, como ya hemos tenido oportunidad de indicar, el Art. 2.1 de la ley, al delimitar su ámbito de aplicación, se refiere a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado, y el Art. 3º, d), al definir al “responsable del fichero”, alude a la persona física o jurídica de naturaleza pública o privada, así como también al órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. Por otra parte, en los ficheros de los que sean responsables las Administraciones Públicas, el Art. 45.2 LORTAD abre la posibilidad, en los supuestos de infracciones contempladas por

33 Pablo Lucas Murillo: “La protección de los datos personales ante el uso de la informática en el Derecho Español”(II), en *Revista Colex*, nº 4, enero-febrero 1993, pp. 7 y sgtes.; especialmente, p. 9.

el Art. 43º de la misma norma legal, de enlazar las sanciones que la ley prevé para sus responsables con la exigencia de responsabilidad disciplinaria. A tal efecto, el Director de la Agencia de Protección de Datos podrá proponer la iniciación de actuaciones disciplinarias respecto de aquellos funcionarios que hubieren infringido sus deberes en perjuicio de los intereses tutelados por la ley, siendo el procedimiento y las sanciones a aplicar los establecidos en la legislación sobre régimen disciplinario de las administraciones públicas.

Como antes dijimos, las personas jurídicas no son sujetos activos de estos derechos, si bien, por el contrario, sí que son incluídas por la LORTAD como sujetos pasivos. Ya aludimos con anterioridad a cómo el Art. 3º, d), al referirse al responsable del fichero, alude a las personas jurídicas de naturaleza pública o privada. Quiere ello decir que los ficheros de personas jurídica de titularidad privada son objeto de las determinaciones de la LORTAD. La salvedad más significativa (Art. 2.2, e/LORTAD) atañe a los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, a cuyos ficheros no les serán de aplicación las normas de la LORTAD. Tampoco lo serán a los ficheros mantenidos por personas físicas con fines exclusivamente personales (Art. 2.2, b/LORTAD).

En las relaciones entre particulares rigen los mismos principios y derechos que en las relaciones que median entre los poderes públicos y los titulares de estos derechos. Sin embargo, a las relaciones entre particulares no se trasladan las numerosas exclusiones de la eficacia de estos derechos que se contemplan en la relación entre un ciudadano y un poder público, circunstancia que ha conducido a algún autor³⁴ a entender que en los ficheros de titularidad privada se garantiza una defensa teórica de la intimidad personal y familiar, de tal suerte que la protección de los datos personales parece completa.

9. Principios de la protección de datos

El Título II de la LORTAD (Arts. 4º al 11º) está dedicado a los prin-

34 Miguel Angel Davara Rodríguez: "La ley española de protección de datos (LORTAD): ¿una limitación al uso de la informática para garantizar la intimidad? (y II)", en *Actualidad Informática Aranzadi*, 19 de noviembre de 1992, pp. 1 sptes.; especialmente, pp. 3 y 4.

cipios de la protección de datos. Estos principios generales definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas, como se reconoce en la Exposición de Motivos de la Ley, a garantizar tanto la veracidad de la información contenido en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, la LORTAD pretende limitar.

El principio del consentimiento, o de autodeterminación, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Este principio se completa a través de la exigencia legal de que al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance.

Hechas estas reflexiones generales, nos centraremos en los principios legales de la protección de datos.

A. El consentimiento del afectado

El principio del consentimiento es la regla capital en esta materia. El Art. 6.1 LORTAD determina que “el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la ley disponga otra cosa”. El propio artículo 6º en su apartado segundo, prevé una excepción a este principio general, por cuanto no será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación de negocio, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

Este consentimiento ha de ser necesariamente expreso y por escrito del afectado en los datos especialmente protegidos (Art. 7.2 LORTAD), pudiendo además ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos (Art. 6.3).

Esta capacidad de autodeterminación o autodisposición sobre la información que a la persona atañe implica que esa persona puede concretar y pronunciarse acerca de los aspectos que no quiere que sean objeto de tratamiento automatizado y de aquellos otros sobre los que no tiene inconveniente en que así acontezca.

Como es lógico, el consentimiento opera decisivamente en el momento de la recogida de los datos. Es lógico por lo mismo que la LORTAD obligue a quien pretenda recoger esa información, a quien desee solicitar datos personales de un ciudadano, a informarle previamente de modo expreso, preciso e inequívoco acerca de los siguientes aspectos (Art. 5.1 LORTAD): a) de la existencia de un fichero automatizado de datos de carácter personal, 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 que le sean 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 y cancelación; y, e) de la identidad y dirección del responsable del fichero. La única salvedad que la ley establece (Art. 5.3) respecto de la necesidad de suministrar esta información se ciñe al supuesto de que el contenido de ella se deduzca claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

B. Los datos especialmente protegidos

Los contornos del principio del consentimiento, como ya hemos señalado, se refuerzan singularmente en los denominados “datos sensibles”, como pueden ser, de una parte, la ideología o creencias religiosas, y de otra, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles, como antes dijimos, con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencias de la LORTAD; ha de fundarse en razones de interés general.

El Art. 7.1 LORTAD reitera la determinación constitucional del Art. 16.2 CE, en el sentido de que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Por lo mismo, cuando se proceda a recabar el consentimiento del afectado en relación con esos datos,

se deberá advertir expresamente al interesado acerca de su derecho a no prestarlo. Por lo demás, como ya hemos advertido con reiteración, sólo previo consentimiento expreso y recogido por escrito por el afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal reveladores de la ideología, religión o creencias.

En cuanto a los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, el Art. 7.3 LORTAD dispone que sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente.

En relación específicamente a los datos atinentes a la salud, la ley (Art. 8º) establece una norma particularizada, al disponer que, sin perjuicio de lo que la propia norma legal prevé en su Art. 11º para la cesión de datos, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con las disposiciones específicas de la Ley Nº 14/1986, de 25 de abril, General de Sanidad; la Ley Nº 25/1990, de 20 de diciembre, del Medicamento, y la Ley Orgánica Nº 3/1986, del 14 de abril, de medidas especiales en materia de Salud Pública.

La LORTAD, en todo caso, impide los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual de los ciudadanos, al prohibirlo expresamente su Art. 7.4.

Se refiere finalmente la ley (Art. 7.5) a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, disponiendo respecto de ellos que sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

C. La calidad de los datos

Como bien dice Lucas Murillo³⁵, aunque el principio del consentimiento es el *prius* para la recogida de datos, consentir ante una solici-

35 Pablo Lucas Murillo: "La protección de los datos personales ante el uso de la informática en el Derecho español", *op. cit.*, p. 19.

tud no supone un apoderamiento general, ilimitado e irreversible en favor de quien ha formulado dicha solicitud. Por el contrario, la LORTAD es bien estricta y, por lo mismo, comienza su Título II ocupándose de esta cuestión (en su Art. 4º), a propósito de lo que ella misma denomina “calidad de los datos”. El Art. 4º viene así a fijar un conjunto de reglas objetivas no sólo sobre los datos, sino también sobre la forma en que han de ser recogidos, utilizados y conservados tanto por los responsables públicos como por los privados. Junto a esas reglas objetivas, el precepto en cuestión establece una serie de vínculos que surten efectos respecto de quienes se dedican al tratamiento automatizado de los datos, vínculos que vienen a ser algo así como el reverso de los derechos de los afectados. Las reglas del Art. 4º LORTAD son las siguientes:

1ª El principio de congruencia entre la finalidad perseguida y la información recabada

A tenor del Art. 4.1 de la ley, sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido. Además, en la clasificación de los datos sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

A su vez, el Art. 4.2 dispone que los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

Una manifestación más de este principio la encontramos en el apartado quinto del Art. 4º de la LORTAD, a cuyo tenor: “Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados”. Complementando esta previsión, el mismo apartado dispone que estos datos de carácter personal no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados

En definitiva, la LORTAD exige una conexión clara y adecuada entre la finalidad legítima que persigue el fichero o el tratamiento y los datos que se requieren de la persona. En sintonía con ello, tales datos

no pueden utilizarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos. Por lo mismo, la desconexión sobrevenida con la finalidad que motivó su captación determina la obligación de cancelar los datos afectados por ella.

2ª El principio de veracidad, exactitud y actualidad de los datos

Los datos han de ser exactos y puestos al día, de forma que respondan con veracidad a la situación real del afectado (Art. 4.3 LORTAD). Esta exigencia pesa, de modo muy especial, sobre los responsables del fichero, sea este público o privado, en cuanto que la Ley (Art. 4.4) obliga a cancelar y sustituir de oficio los datos de carácter personal registrados cuando estos resultaren ser inexactos, en todo o en parte, o incompletos. En tales casos, la sustitución de oficio se hará por los correspondientes datos rectificadas o completados, y ello siempre sin perjuicio del derecho de rectificación y cancelación que la ley reconoce en su Art. 15º a los afectados.

3ª Forma de almacenar los datos

Algunas reglas relacionadas con la calidad de los datos también se ocupan de la forma en que deben almacenarse las informaciones personales recogidas. Ya hemos dicho que el Art. 4.1, *in fine*, dispone que en la clasificación de los datos sólo podrán utilizarse criterios que no se presten a prácticas ilícitas. Tampoco podrán ser conservados, como también señalamos con anterioridad, en forma tal que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados (Art. 4.5). Finalmente, los datos serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del interesado (Art. 4.6).

4ª Interdicción de la recogida de datos ilícita

El apartado séptimo del Art. 4º de la LORTAD prohíbe taxativamente la recogida de datos por medios fraudulentos, desleales o ilícitos.

5ª El derecho al olvido

Lucas Murillo³⁶ habla de la existencia en la LORTAD de una suerte de derecho al olvido. Quien consiente que aspectos relativos a su persona puedan ser incorporados a un fichero informático y ser objeto de elaboración con vistas a su utilización en un sentido específico, puede delimitar temporalmente su autorización, tal y como ya advertimos, fijando un plazo determinado o determinable transcurrido el cual recupera la plena disposición sobre la información que le concierne, debiendo producirse entonces la cancelación de los registros que la contuviera. En tal sentido, el Art. 15.5 LORTAD dispone que los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado.

La propia LORTAD (Art. 28º) establece un plazo para el registro y cesión de datos personales, al circunscribir los que pueden registrar y ceder los ficheros privados sobre la solvencia patrimonial y el crédito. En concreto, aquellos que sean adversos a la hora de determinar la solvencia económica de una persona, a tenor del citado precepto legal, no pueden remontarse a más de seis años.

Por lo demás, ya hemos visto cómo, mediando una causa justificada, el consentimiento prestado puede ser revocado si bien tal revocación no puede operar retroactivamente. Asimismo, también hemos visto que el Art. 4.5 LORTAD ordena la cancelación de los datos de carácter personal cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

D. Seguridad de los datos

La LORTAD dedica uno de sus preceptos (Art. 9º) a la seguridad de los datos, previniendo al respecto que el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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.

³⁶ *Ibidem*, pp. 21-22.

De igual forma, se establece (Art. 9.2) que no se registrarán datos de carácter personal en ficheros automatizados 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 tratamiento, locales, equipos, sistemas y programas.

Finalmente, la ley se remite a la ordenación reglamentaria a los efectos del establecimiento de los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los “datos sensibles” a que se refiere el Art. 7º de la propia ley.

E. Deber de secreto

El Art. 10º LORTAD prevé de modo específico un deber de secreto que afecta al responsable del fichero automatizado y a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal. Todos ellos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligación que subsiste aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

F. Cesión de datos

Para la adecuada salvaguarda de los derechos de la personalidad a que se refiere la LORTAD, resulta esencial la correcta regulación de la cesión de los datos almacenados. Como se admite en la Exposición de Motivos de la Ley, es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el perfil personal de un individuo, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la ley completa el principio del consentimiento, exigiendo que, al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance.

De conformidad con el Art. 11.1 LORTAD, los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consenti-

miento del afectado. Este consentimiento, que tiene carácter revocable (Art. 11.4), será nulo cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente (Art. 11.3 LORTAD). Por otro lado, el cesionario de los datos de carácter personal se obliga, por el sólo hecho de la cesión, a la observancia de las disposiciones de la LORTAD (Art. 11.5).

El consentimiento exigido por el Art. 11.1 para la cesión no es preciso, de conformidad con el apartado segundo del mismo Art. 11°, en los siguientes casos: a) cuando una ley prevea otra cosa; b) cuando se trate de datos recogidos de fuentes accesibles al público; c) cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros; d) cuando la cesión que deba efectuarse tenga por destinatarios el Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales, en el ejercicio de las funciones que tienen atribuidas; e) cuando la cesión se produzca entre las administraciones públicas en los supuestos contemplados por el Art. 19° de la ley; y, f) cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos por la Ley General de Sanidad.

10. Los derechos de las personas

Las garantías de la persona son, como bien se afirma en la Exposición de Motivos de la Ley, los nutrientes nucleares de la parte general de la norma, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios generales. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general de la ley, a los que ya nos hemos referido, principios que, parece evidente, sin los derechos subjetivos que ahora analizaremos, no rebasarían un contenido meramente programático. En concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se convierten en las piezas centrales del sistema cautelar o preventivo instaurado por la LORTAD.

Nos referiremos a continuación a cada uno de estos derechos, de modo particularizado.

A. El derecho de información

El Art. 13° LORTAD determina que cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos (órgano integrado en la Agencia de Protección de Datos en el que han de inscribirse, entre otros, todos los ficheros automatizados de propiedad pública o privada), la existencia de ficheros automatizados de datos de carácter personal, como también sus finalidades y la identidad del responsable del fichero. Esta consulta, como cualquier otra realizada ante el citado Registro, será pública y gratuita.

Como bien señala la doctrina³⁷, el Registro es un medio indispensable para conocer de donde proceden los riesgos potenciales para los derechos de las personas y ejercer las medidas preventivas y, si es el caso, represivas que se hagan necesarias.

B. El derecho de acceso

El Art. 14° de la ley contempla este derecho capital, al reconocer al afectado el derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados. La información puede consistir en la mera consulta por medio de su visualización, o en la comunicación de los datos pertinentes (es decir, de todos los que atañen a tal persona) mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.

El acceso ha de poner de relieve asimismo, aunque no se contemple de modo explícito por el Art. 14°, las cesiones que han hecho de los datos del afectado a terceros, así como la identidad del cesionario y la finalidad que éste persigue. Y ello ha de ser así aunque el Art. 25° LORTAD exija asimismo que el responsable de un fichero, en el momento en que se efectúe una primera cesión de datos, debe informar de

37 Pablo Lucas Murillo: "La protección de los datos personales ante el uso de la informática en el Derecho español" (II), *op. cit.*, p. 26.

ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

A partir del Convenio núm. 108 del Consejo de Europa, tantas veces citado (cuyo Art. 8º, b), recordémoslo, reconoce el derecho de cualquier persona a obtener a intervalos razonables y sin demora o gastos excesivos, la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible), el Derecho comparado nos revela que puede exigirse un canon o contraprestación no excesivo (esto es, razonable) por este acceso. La LORTAD no se pronuncia al efecto, bien que su Art. 16.2 deja abierta esta posibilidad por la vía reglamentaria, en cuanto que limita la no exigencia de contraprestación alguna a los supuestos de rectificación o cancelación de los datos de carácter personal inexactos.

En sintonía con el Convenio núm. 108 del Consejo de Europa (que, como acabamos de ver, habla de “intervalos razonables”), el Art. 14.3 de la ley determina que el derecho de acceso sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

El procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente, tal y como prevé el Art. 16.1 LORTAD.

C. El derecho de rectificación

Este derecho de rectificación, como es lógico, se dirige a obtener la corrección o integración de aquellos datos que figuren de manera inexacta o incompleta en un fichero. Como es obvio, está llamado asimismo a posibilitar la actualización de la información que se haya visto desfasada.

El Art. 15.1 de la ley dispone que el responsable del fichero tendrá la obligación de hacer efectivo, en el plazo que reglamentariamente se establezca, el derecho de rectificación, habiendo de ser rectificadas (Art. 15.2) los datos de carácter personal que resulten inexactos o incompletos. Si los datos rectificados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación efectuada al cesionario (Art. 15.3).

Ya hemos señalado con anterioridad que, a tenor del Art. 16.2 LORTAD, no podrá exigirse canon o contraprestación alguna por la rectificación de los datos de carácter personal inexactos.

D. El derecho de cancelación

Tiene este derecho por objeto eliminar del fichero aquellos datos personales que ya no deban figurar en él, bien porque nunca debieron ser registrados, bien porque, habiendo sido recogidos legalmente, alguna causa exija su supresión.

El propio Art. 15° LORTAD acoge, conjuntamente con el derecho de rectificación, el de cancelación, determinando la obligación del responsable del fichero de hacer efectivo, en el plazo reglamentariamente previsto, el derecho de cancelación del afectado. Los datos de carácter personal que resulten inexactos o incompletos serán, en su caso, cancelados. Si los datos cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la cancelación efectuada al cesionario.

Recordemos que el Art. 4.4 LORTAD, como ya vimos, establece un supuesto de cancelación de oficio de aquellos datos de carácter personal registrados que resultaren ser inexactos, en todo o en parte, o incompletos. Ello debe ponerse en conexión con el Art. 15.2, que recoge el derecho del interesado a la cancelación, también en los supuestos de de datos incompletos o inexactos.

En cuanto al plazo, es preciso señalar que, transcurrido el que contemplaba la autorización del afectado, o la disposición normativa que permitía su recogida (recordemos la previsión legal ya comentada sobre los ficheros de titularidad privada relativos a la solvencia y al crédito patrimonial), o dándose la circunstancia prevista en el párrafo segundo del Art. 4.5 LORTAD (es decir, cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la que fueron recabados y registrados), deberá procederse a su cancelación de oficio y, desde luego, a requerimiento del titular del derecho. Como bien advierte Lucas Murillo³⁸, esta interpretación puede entresecarse, a *contrario sensu* del Art. 15.5 de la ley, pues al indicar en qué circunstancias deben conser-

38 *Ibidem*, p. 29.

varse los datos (los datos deben ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado), abre el derecho a exigir su cancelación en todos los demás supuestos.

Finalmente, el Art. 15.4 LORTAD establece un supuesto en el que no procede la cancelación: cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos. Parece una necesaria evidencia entender que la primera de esas causas sólo ha de venir referida a la cancelación de oficio, no a la instada por la persona a la que conciernen los datos, pues carece de toda lógica pensar que la defensa del afectado deba hacerse contra su voluntad. En cuanto a la tercera de las causas, Lucas Murillo³⁹, con buen criterio, cree que esa obligación de conservar los datos ha de derivar expresamente de una ley que, también, ha de ser orgánica. Y ello porque si nos hallamos en el ámbito de un derecho fundamental, no basta para limitarlo ni una mera norma administrativa, ni tampoco una ley ordinaria.

E. El derecho a impugnar los actos o decisiones que impliquen valoraciones basadas exclusivamente en datos automatizados

El Art. 12º LORTAD reconoce el derecho de la persona afectada a impugnar los actos administrativos o las decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Se trata, pues, de reaccionar jurídicamente, a través de esta vía impugnatoria, frente a aquellas situaciones en las que, como ya señalamos haciéndonos eco de la Exposición de Motivos de la propia ley, a partir de datos de diferente naturaleza, se diseña un perfil personal de un individuo determinado, cuya obtención, como también dijimos, transgrediría los límites de la privacidad.

Y es que lo que claramente parece querer rechazar el legislador al perfilar en el Art. 12º este derecho de impugnación, es que un acto

39 *Ibidem*, p. 30.

administrativo o una decisión privada que sean perjudiciales para una persona tengan como único fundamento la valoración de esa misma persona verificada por una concreta elaboración informática. Se trataría, como dice Lucas Murillo⁴⁰, de proteger la autodeterminación informativa en un aspecto fronterizo con el honor. No es tanto el menoscabo de la estima y consideración que cada uno debe merecer lo que pretende combatir el Art. 12º, sino el que una reconstrucción artificial del perfil personal de un individuo le depare perjuicios en sus relaciones públicas o privadas.

F. Tutela de los derechos y derecho de indemnización

El Art. 17º LORTAD contempla los mecanismos procesales con los cuales hacer frente a las actuaciones contrarias a lo dispuesto en la propia Ley.

El primero de esos cauces procesales consiste en la reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

Si se nos permite el *ex cursus*, la Agencia de Protección de Datos, que crea la LORTAD (a la que dedica su Título VI), es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Se rige por lo establecido por la propia ley y por un Estatuto aprobado por Real Decreto Nº 428/1993, del 26 de marzo, modificado por otro Real Decreto, el Nº 156/1996, del 2 de febrero. Al frente de la Agencia se encuentra la figura de su Director, nombrado de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. A su vez, el Consejo Consultivo, de conformidad con el Art. 37º LORTAD, se halla compuesto por los siguientes miembros: a) un Diputado, propuesto por el Congreso; b) un Senador, propuesto por el Senado; c) un representante de la Administración Central, designado por el Gobierno; d) un representante de la administración local, propuesto por la Federación Española de Municipios y Provincias; e) un miembro de la Real Academia de la Historia, propuesto por la misma;

40 *Ibidem*, p. 31.

f) un experto en la materia, propuesto por el Consejo Superior de Universidades; g) un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente; h) un representante de las Comunidades Autónomas, cuya propuesta se realizará a través del procedimiento que se establezca en las disposiciones de desarrollo de la LORTAD; y, finalmente, i) un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

La Agencia de Protección de Datos bien puede considerarse una garantía institucional del conjunto de los derechos previstos por la LORTAD.

El procedimiento de reclamación de los afectados ante la Agencia ha sido regulado por el Art. 17º del Real Decreto N° 1332/1994, del 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica N° 5/1992. Tal procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica N° 5/1992 que se consideren vulnerados.

Recibida la reclamación en la Agencia, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

Recibidas las alegaciones o transcurrido el plazo anteriormente referido, la Agencia de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada, dando traslado de la misma a los interesados.

Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

El segundo de los cauces procesales a que venimos refiriéndonos atañe, tras el reconocimiento que el Art. 17.3 de la ley hace del derecho de indemnización de los afectados que, como consecuencia del incumplimiento de las determinaciones legales, sufran daño o lesión en sus bienes o derechos, a la responsabilidad que hubieren podido contraer los sujetos pasivos. La Ley abre aquí dos vías diferenciadas según se trate (Art. 17.4) de ficheros de titularidad pública o de ficheros de titularidad privada (Art. 17.5). En el primer caso, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las administraciones públicas, es decir, según la normativa

prevista por la Ley N° 30/1992, del 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En el segundo supuesto, la acción se ejercitará ante los órganos de la jurisdicción ordinaria, o lo que es igual, ante la jurisdicción civil.