El Derecho a la autodeterminación informativa en la ley portuguesa de protección de datos de 1991. Sujetos, contenido y garantías

JOSE M.ª ASPAS ASPAS
Licenciado en Derecho
Administrador Superior
Diputación General de Aragón
(ESPAÑA)

SUMARIO

B) Almacenamiento y tratamiento automatizado de datos.

C) Transmisión.

D) Obligaciones del sujeto pasivo.

3. Garantías.

A) Garantías institucionales. La CNPDPI.

B) Delitos y sanciones.

I. LA CONSTITUCIONALIZACION DE LA PROTECCION DE DATOS FRENTE A LA INFORMATICA

El artículo 35 de la Constitución de la República de Portugal de 1976 (CRP) establece lo siguiente:

«1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.

2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.

3. Queda prohibida la atribución de un número nacional único a los ciudadanos» [1].

De este modo Portugal es el primer Estado europeo que constitucionaliza la protección de datos personales frente al uso de la informática [2]. El derecho de acceso, el derecho a conocer la finalidad a la que se destinan los datos, el derecho de rectificación, la prohibición de captar datos sensibles y la prohibición del número de identificación personal único son elementos de la técnica de protección de datos personales conocidos en la legislación comparada de protección de datos [3] de los

---

[1] Citamos por la traducción de M. Daranas publicada en el *Boletín de Legislación Extranjera*, núm. 206 (1976), reproducida por J. De Esteban: *Constituciones españolas y extranjeras*, Taurus, 2.ª ed., Madrid, 1979.

[2] Sobre el artículo 35 de la Constitución portuguesa vid. R. Capelo de Sousa: «A Constituição e os direitos da personalidade» en la obra colectiva *Estudos sobre a Constituição, II*, Lisboa, 1978, pp. 194 y ss. y J. J. Gomes Canotilho y V. Moreira: *Constituição da República Portuguesa. Anotada*, Coimbra Editora, 1980, pp. 103-104.

[3] La expresión «protección de datos es una importación de la terminología alemana *(Datenschutz)* y anglosajona *(Data protection)* con aceptación entre la doctrina española y comparada. Con ella se alude a las normas jurídicas de diverso rango (internacional, constitucional, legal o reglamentario) cuya finalidad es la tutela de bienes jurídicos o derechos de las personas que puedan ser afectados por la elaboración informática de informaciones referentes a personas. Es, por tanto, una expresión equívoca, porque estas disposiciones pretenden proteger a las personas concernidas por los datos, pero no son objeto de protección jurídica los datos por sí mismos. Sobre la cuestión terminológica *cfr.* A. E. Pérez Luño: «Los derechos humanos en la sociedad tecnológica» en M. G. Losano, A. E. Pérez Luño, Mª F. Guerrero Mateus, *Libertad informá-*

años setenta, pero que con su constitucionalización ejercerán una influencia sobre otros sistemas jurídicos [4].

Con el reconocimiento de esa serie de facultades a los ciudadanos para la protección de su identidad informativa, la Constitución portuguesa no constitucionaliza *expressis verbis* el derecho a la autodeterminación informativa,[5] pero lo dota de un contenido mínimo o esencial que no puede ser ignorado por el legislador ordinario.

II. EL DESARROLLO LEGISLATIVO DEL ARTICULO 35 DE LA CONSTITUCION

1. El retraso legislativo. Compromisos internacionales.

Quince años han transcurrido entre la aprobación de la Constitución y el desarrollo legislativo de su art. 35. En efecto, la Ley 10/91, *Ley de protección de datos personales frente a la informática* (LPDP), publicada en el Diario de la República, I Serie-A, n.º 98, de 29 de abril de 1991, llena el vacío legislativo del ordenamiento jurídico portugués en materia de protección de los datos personales [6].

La Ley portuguesa de 1991 debe su aprobación a dos compromisos internacionales. En primer lugar, el *Convenio para la protección de las personas*

---

tica y leyes de protección de datos personales, CEC, Madrid, 1989.

[4] El art. 35 CRP es el antecedente del art. 18.4 de la Constitución española. *Vid* J.M. SERRANO ALBERCA: «Comentario al art. 18», en F. GARRIDO FALLA, *Comentarios a la Constitución*, Civitas, 2.ª ed., Madrid, 1985, pp. 351 - 381 y J. GALVEZ MONTES: «Derecho al honor, a la intimidad y a la propia imagen. Comentario al art. 18 de la Constitución», en O. ALZAGA, *Comentarios a las leyes políticas. Constitución española*, t. II, Edersa, Madrid, 1984.

[5] El derecho a la autodeterminación informativa o libertad informática es una construcción jurisprudencial y doctrinal. Fue enunciado por el Tribunal constitucional alemán (sentencia de 15 de diciembre de 1983, sobre la Ley del censo de 31 de marzo de 1982) hay traducción castellana BJC 33 (1984), pp. 126 y ss como un derecho ligado al derecho a la personalidad (art. 2.1 GG). La doctrina ha intentado configurarlo como un derecho autónomo, correspondiente a la tercera generación de derechos fundamentales. *Vid* A. E. PÉREZ LUÑO: «Libertad informática y derecho a la autodeterminación informativa» en AA.VV., *Congreso sobre Derecho Informático. Texto de ponencias y comunicaciones. Edición previa*, 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 359-376. También P. LUCAS MURILLO DE LA CUEVA: *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Tecnos, Madrid, 1990.

[6] Tras la aprobación de la Ley portuguesa, en ámbito de los países europeos, sólo carecen de ley de protección de datos tres países: España, Italia y Portugal. En caso de España, se encuentra muy avanzada la tramitación parlamentaria del *Proyecto de Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal (BOCG-CD*, Serie A, núm. 59-1, de 24-7-1991 y *BOCG-S*, Serie II núm. 80(a), de 1-6-1992). Italia carece de una ley específica de protección de datos: se han planteado diversas propuestas para colmar esta laguna, de las que da noticia M. G. LOSANO: «Un proyecto de ley sobre la protección de los datos personales en Italia», en M. G. LOSANO, A. E. PÉREZ LUÑO, M.ª F. GUERRERO MATEUS, *Libertad informática y leyes de protección de datos personales*, cit., pp. 61-94.

con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. El Convenio 108 del Consejo de Europa vincula a los Estados que lo han ratificado, aceptado o aprobado[29]

En segundo lugar, el *Convenio de aplicación del Acuerdo de Schengen* de 14 de junio de 1985 entre el Benelux, Alemania y Francia, *relativo a la supresión gradual de controles en las fronteras comunes*, firmado en Schengen el 19 de junio de 1990,[30] al cual se adhirió, en junio de 1991, Portugal. La adhesión le obligaba a adoptar, antes de la ratificación, todas las iniciativas necesarias para que la legislación portuguesa fuese completada de conformidad con el Convenio 108 del Consejo de Europa.

El Convenio de aplicación del Acuerdo establece en su título IV (arts. 92-119) un sistema de información común, denominado *Sistema de Información de Schengen*. Este sistema consiste en la creación y mantenimiento de un fichero de datos por cada parte contratante y la creación de una unidad de apoyo técnico, que haga posible la consulta automatizada de datos sobre personas y objetos para la aplicación de las disposiciones relativas a la circulación de las personas. Además, se establecen disposiciones sobre la protección de datos de carácter personal (arts. 126-130). Las partes contratantes se obligan a adoptar las disposiciones nacionales que sean necesarias para conseguir un nivel de protección de los datos de carácter personal que sea, al menos, igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (art. 126.1), sin que puedan transmitirse datos de carácter personal, según el Convenio, hasta que las disposiciones de protección de datos hayan entrado en vigor en el territorio de la parte contratante afectada por la transmisión (art. 126.2).

En nuestra opinión, la adhesión de Portugal al Convenio de aplicación del Acuerdo de Schengen es la causa inmediata del desarrollo legislativo de

[29] En 1988, de los veintiún Estados miembros del consejo de Europa, ocho habían ratificado el Convenio 108 (Austria, Francia, España, Luxemburgo, Noruega, R.F. de Alemania y Suecia); otros diez habían expresado mediante su firma su voluntad de ratificarlo (Bélgica, Chipre, Dinamarca, Grecia, Irlanda, Italia, Islandia, Países Bajos, Portugal y Turquía). *Vid* S. RIPOL CARULLA: «El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: balance a los siete años de su apertura a la firma» en AA.VV., *Congreso sobre Derecho Informático. Textos de ponencias y comunicaciones. Edición previa*, 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 395-413.

[30] El texto del Convenio de aplicación de 1990 del Acuerdo de Schengen puede consultarse en el *BOCG-CD*, Series C, núm.194-1 de 26-10-1991. Además de los cinco Estados iniciales, forman parte Italia, que se adhirió en noviembre de 1990 y, España y Portugal, que se adhirieron en junio de 1991; Grecia participa desde enero de 1992 como observador. Sobre el citado Acuerdo, *cfr.* J. L. CRUESUMBRA: «Las fronteras de la Comunidad Europea» y J. ELORZA: «Libre circulación de personas», ambos trabajos publicados en AA.VV., *El mercado único. La Europa sin fronteras interiores*, Acción Institucional 93, Secretaría de Estado para las Comunidades Europeas, Madrid, 1992, pp. 111-119 y 131-141, respectivamente.

la protección de datos prevista en el art. 35 de la Constitución, demorado durante tres lustros.

Como hemos señalado, el Convenio de aplicación del Acuerdo de Schengen establece como parámetro de la protección de los datos personales los principios del Convenio 108 del Consejo de Europa. LUCAS MURILLO DE LA CUEVA ha sintetizado dichos principios, aplicables al sector público y privado, en los siguientes: principio de lealtad, de exactitud, finalista (que comprende los principios de pertinencia, de utilización no abusiva, del derecho al olvido), de publicidad, de acceso individual, de seguridad, la prohibición de tratar informáticamente datos sensibles, salvo que el Derecho interno prevea garantías adecuadas, el establecimiento de recursos y sanciones para garantizar los anteriores principios y, por último, la prohibición de transmitir datos personales a países que no les den una protección equivalente[9].

2. La Ley 10/91. Ley de protección de datos personales frente a la informática.

La LPDP tiene una extensión de 45 artículos, distribuidos en nueve capítulos. El principio inspirador de la regulación de la Ley es el establecimiento de un sistema *preventivo* frente a los riesgos que comporta el uso informático de datos personales sin un control por las personas concernidas por ellos [10]. Las actividades de captación, conservación, tratamiento y transmisión automatizada de datos personales sólo pueden hacerse de acuerdo con las previsiones de la Ley. Es decir, no es un régimen jurídico de libertad incondicionada, sino que la Ley fija el régimen preciso al que deben someterse los agentes que utilizan la informática [11].

La precisión técnica implica la necesidad de incorporar definiciones legales. Así el art. 2 de la LPDP define lo que se entiende, a efectos legales, por datos personales, datos públicos, sistema informático, fichero automatizado, base de datos, banco de datos, tratamiento automatizado, responsable de los soportes informáticos, flujo de datos transfronterizos [12]. Quizás la Ley

---

[9] P. LUCAS MURILLO DE LA CUEVA: *El derecho a la autodeterminación informativa, cit. pp. 141-144.* También A. E. PÉREZ LUÑO «Los derechos humanos en la sociedad tecnológica», *cit.* pp. 163-184.

[10] A juicio de M. HEREDERO HIGUERAS es más eficaz un sistema preventivo de actuación que un sistema *ex post facto*, aunque también es posible éste. *Vid.* «Ante la ratificación del Convenio de protección de datos del Consejo de Europa», DA 199 (1983), p. 762 y «El anteproyecto de ley orgánica de regulación del uso de informática, cinco años después» en AA.VV., *Congreso sobre Derecho informático. Texto de ponencias y comunicaciones. Edición previa*, 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, p. 276.

[11] *cfr.*, p. ej., los arts. 17 (requisitos de creación de ficheros automatizados), 24 (interconexión de datos personales) y 32 (flujo transfronterizo de datos). P. LUCAS MURILLO DE LA CUEVA defiende que el principio inspirador de una ley de protección de datos debe ser la fijación de un marco jurídico preciso. *Vid.* «La protección de los datos personales ante el uso de la informática, *RFDUC* 15 (1990), p.615 y *El derecho a la autodeterminación informativa, cit. pp.178 179.*

[12] *Cfr.*, el art. 2 del Convenio 108 del Consejo de Europa. Las definiciones del Convenio sólo se refieren a datos de carácter personal, ficheros automatizados, tratamiento automatizado,

no debería hacer referencia expresa a las locuciones «banco de datos», «base de datos» o «sistema informático», ya que son conceptos que están vinculados a un determinado estadio del desarrollo informático y de la evolución tecnológica de la informática [13].

Como hemos señalado *supra*, el art. 35 de la Constitución no recoge el bien jurídico protegido, es decir, la autodeterminación informativa, sino diversas técnicas de protección de datos. Sin embargo, la LPDP, al señalar el objeto y fin de la regulación, ha precisado el bien jurídico protegido. El art. 1 de la Ley establece:

«El uso de la informática debe procurarse de forma transparente y con estricto *respeto* a la *reserva de la vida privada y familiar* y de los *derechos, libertades y garantías fundamentales* del ciudadano.»

Este artículo no se refiere exclusivamente a la reserva personal y familiar (o intimidad), sino también a los derechos, libertades y garantías fundamentales de los ciudadanos. Además de la intimidad personal y familiar hay otros bienes jurídicos que deben tenerse en cuenta. La autodeterminación informativa como derecho fundamental autónomo guarda relación de complementariedad con otros derechos y libertades fundamentales, como son la de conciencia, religión y culto (art. 41 CRP), la de expresión y de información (art. 37).

El bien jurídico protegido es la identidad informativa, manifestación de la *identidad de la persona*.[14] Lo que se protege es el control de la utilización y tratamiento automatizado de datos personales por las personas afectadas.

Es importante destacar la perspectiva que adopta la LPDP: lo que se regula es el uso de la informática (art. 1). Este enfoque ya estaba presente en el art. 35 de la Constitución, que lleva por título «*Utilización de la informática*». Se pretende resolver el conflicto entre la libertad de utilizar sistemas automáticos de almacenamiento, tratamiento y transmisión de datos personales y la libertad informática o autodeterminación informativa. Por ello, se regula el uso, sometiéndolo al régimen legal que configura el *status* de *habeas data*[15], concretado en las garantías o derechos de acceso y control de las informaciones procesadas informáticamente por las personas concernidas.

---

autoridad controladora del fichero. La LPDP ha incluido, además, las definiciones de los datos públicos, sistema informático, base de datos, banco de datos y flujo transfronterizo.

[13] El término «fichero automatizado», que es el que utiliza el Convenio europeo, bastaría para englobar los conceptos de base y banco de datos. Esta simplificación terminológica haría menos redundante el texto de la Ley, ya que en la mitad de sus artículo -concreto en los arts. 3, 8, 13, 14, 17, 18, 20, 21, 24, 25, 26, 27, 29, 32, 34, 35, 36, 37, 39, 40, 41, 44, y 45- se repite la expresión «fichero de datos, base de datos y banco de datos».

[14] M. HEREDERO HIGUERAS («Ante la ratificación del Convenio de protección de datos del Consejo de Europa», *cit.*, p. 762) sostiene que lo que debe ser protegido por las leyes de protección de datos es «la integridad de la información personal, en cuanto que es expresión de la identidad de la persona. El tráfico incontrolado de la información personal puede dar lugar a distorsiones o alteraciones de la identidad de las personas».

[15] Sobre el *habeas data vid.* A. E. PÉREZ LUÑO: «Del *habeas corpus* al *habeas data*»

III. ELEMENTOS DEL DERECHO A LA AUTODETERMINACION INFORMATIVA EN LA LEY PORTUGUESA DE PROTECCION DE DATOS PERSONALES

El derecho a la autodeterminación informativa es una posición jurídica subjetiva que corresponde al *status* de *habeas data*. Es, valga la redundancia, un derecho subjetivo, configurado por la Constitución y por la Ley de protección de datos personales de 1991.

1. Elementos subjetivos.

El derecho a la autodeterminación informativa implica la existencia de una relación jurídica con dos sujetos o posiciones: la del titular del derecho (posición activa) y la de los obligados (posición pasiva).

A) Sujeto activo.

El titular del derecho a la autodeterminación informativa es, en primer lugar la *persona física. La dicción literal del artículo 35 de la Constitución plantea un problema al limitar la protección a los ciudadanos* («Todos los ciudadanos...»). La Ley, siguiendo la senda constitucional, refiere el derecho a la autodeterminación informativa a los ciudadanos (art. 1). No obstante, hay que entender que la protección se extiende a los *extranjeros*, como titulares del derecho, en virtud del art. 15 de la Constitución, ya que ni ésta ni la Ley han reservado este derecho exclusivamente a los ciudadanos portugueses [16].

En segundo lugar, también son titulares del derecho las *personas jurídicas*, siempre que los ficheros, bases o bancos de datos contengan datos personales. Así resulta del art. 3.1.h) de la Ley, que dice: «Las disposiciones de la presente Ley se aplicarán obligatoriamente: (...) a los soportes informáticos relativos a personas jurídicas y entidades equiparadas, siempre que contengan datos personales». El Convenio del Consejo de Europa se refiere a las personas físicas (art. 1), pero deja abierta la posibilidad de que los Estados miembros puedan extender el régimen de protección a las personas jurídicas (art. 3.b.). Esta extensión de la titularidad del derecho a la autodeterminación informativa a las personas jurídicas, que ha efectuado el legislador portugués, es una clara manifestación de que el bien jurídico protegido no es exclusivamente la intimidad personal o familiar, ya que ésta en sentido estricto, sólo podría referirse a las personas físicas y a los miembros individuales de las personas jurídicas [17].

---

en AA.VV., *Encuentros sobre Informática y Derecho 1990-1991*, Universidad Pontificia de Comillas, Madrid, 1992, pp.171-179.

[16] El art. 15 CRP dispone: «1. Los extranjeros y los apátridas que se encuentren o residan en Portugal gozarán de los derechos y estarán sujetos a los deberes del ciudadano portugués. 2. Quedan exceptuados de lo dispuesto en el número anterior (...) los derechos y deberes reservados por la Constitución y por la ley a los ciudadanos portugueses».

[17] Sobre el problema de las personas jurídicas *vid* P. LUCAS MURILLO DE LA CUEVA «La

B) Sujeto pasivo.

El sujeto pasivo del derecho a la autodeterminación informativa configurado por la LPDP es toda *persona física o jurídica, pública o privada*, que utilice sistemas de almacenamiento y tratamiento automatizado de datos personales.

La extensión de la posición pasiva deriva del art. 17 de la Ley que, al determinar los requisitos a los que está sujeta la creación de ficheros automatizados, bases o bancos de datos, somete al régimen legal a todos los sujetos que creen ficheros, sean entidades públicas o privadas. Las amenazas a la identidad informativa pueden proceder del sector público y también del sector privado: por ello, el derecho a la autodeterminación informativa no se configura como un derecho público subjetivo, sino como un derecho subjetivo en el que pueden ocupar la posición de deber las personas públicas y las privadas.

El *ámbito de aplicación* de la LPDP delimitado en su art. 3 determina que a su régimen legal se sujeten únicamente los ficheros automatizados, quedando excluidos los manuales. Además, se excluyen una serie de supuestos en los que media el consentimiento implícito de la persona concernida (procesamiento de remuneraciones, facturación de suministros, cobro de cotizaciones) y los ficheros que contienen datos personales destinados a mantener la seguridad pública (Sistema de Información de la República). También se excluyen los ficheros que contengan informaciones destinadas al uso personal. Respecto a los datos relacionados con la seguridad pública, el art. 9.2 del Convenio 108 del Consejo de Europa permite dicha exclusión.

2. Contenido del derecho.

El contenido del derecho a la autodeterminación informativa se desprende de las facultades que la LPDP atribuye al sujeto activo para proteger su identidad informativa. Es el conjunto de derechos subjetivos que permiten al sujeto activo definir la intensidad con la que desea que sea conocida su identidad informativa, circulen sus datos y que, además, le permitan defenderse de los abusos, inexactitudes o uso desviado que de los mismos se haga, bien sea en el momento de su recogida, tratamiento, almacenamiento o transmisión.

A) Recogida de datos.

El art. 22 de la Ley establece que la recogida de datos personales debe hacerse mediante un *documento o cuestionario, en el que debe constar que los datos serán procesados automáticamente, si es obligatorio o facultativo*

---

protección de los datos personales ante el uso de la informática, *cit.* pp. 617-618 y la reelaboración posterior, *El derecho a la autodeterminación informativa, cit.* pp. 181-182, en la que modifica su criterio.

proporcionar los datos, las consecuencias en caso de omisión o inexactitud de las respuestas, los destinatarios de las informaciones, su finalidad, la identificación del responsable del fichero y su dirección y las condiciones del ejercicio del derecho de acceso. Sin embargo, estos requisitos no se exigen en la recogida de datos destinados a la prevención de delitos o con fines estadísticos (art. 22.2).

Esencial en la técnica de protección de datos referida a su captación es la prohibición de recoger *datos personales sensibles*. Esta prohibición es un mandato del art. 35.2 de la Constitución y ha sido completada por el art. 11 de la Ley. La Constitución prohíbe el tratamiento automatizado de datos referentes a las convicciones políticas, fe religiosa o vida privada. A estas categorías de datos la Ley ha añadido las referidas a la filiación política o sindical (art. 11.1.a.) y al origen étnico, condenas penales, sospechas de actividades ilícitas, estado de salud y situación patrimonial y financiera (art. 11.1.b.).

La prohibición constitucional pese a la rotundidad de los términos en los que está formulada, no debe entenderse de una forma absoluta. Así lo ha interpretado el legislador, que permite el tratamiento de los datos sensibles si media el consentimiento previo de sus titulares, con el conocimiento por éstos del destino y utilización de los datos (art. 11.4).

Por otra parte, el tratamiento de datos sensibles enumerados en la letra b) del art. 11.1 (esto es, los añadidos por la Ley) puede ser efectuado por los servicios públicos, siempre que se respete el régimen legal y se cuente con el parecer de la Comisión Nacional de Protección de los Datos Personales Informatizados (art. 11.3), que la Ley crea.[18] Por lo tanto, se establece una «escala de informaciones sensibles».

Si los datos sensibles no son identificables pueden ser objeto de tratamiento automatizado para fines de investigación o estadísticos (art. 11.2). Esta modulación o relativización de la prohibición es consecuencia de dos hechos: uno, que los datos sensibles dejan de serlo si no es identificada o identificable la persona a la que se refieran; es más, dejan de ser, a efectos legales, datos personales (*cfr.* la definición de los datos personales de la letra a) del art. 2 LPDP); el otro hecho es que la perspectiva de la legislación de protección de datos es regular la utilización de la información, de ahí que determinados usos (investigación científica o estadística) sean permitidos.

En la recogida de datos rige el principio de calidad de los datos, reconocido en el art. 5 del Convenio 108 del Consejo de Europa. Así, los datos personales que sean objeto de tratamiento automatizado deben cumplir los requisitos de: *lealtad*, la recogida debe efectuarse de forma lícita y no engañosa (art. 12.1 LPDP); *finalidad*, la finalidad determinante de la recogida

[18] A la CNPDPI nos referiremos *infra* §III.3.A).

debe ser conocida antes de su inicio (art. 12.3); *pertinencia*, la recogida debe procesarse con estricta adecuación y pertinencia a la finalidad que se determine (art. 12.2); y, *exactitud*, los datos personales recogidos y mantenidos en ficheros automatizados deben ser exactos y actuales (art. 35.1 CRP y art. 14 LPDP).

B) Almacenamiento y tratamiento automatizado de datos.

El sujeto activo del derecho a la autodeterminación informativa goza de una serie de derechos para defender su posición. Así,

a) El *derecho a conocer la existencia* de bancos de datos. El art. 13 LPDP establece que cualquier persona tiene el derecho de ser informada sobre la existencia de un fichero automatizado, base o banco de datos personales que le afecten, de la respectiva finalidad, así como sobre la identidad y la dirección del responsable. Es un principio paralelo al recogido en el art. 8 del Convenio del Consejo de Europa.

b) El *derecho de acceso* a la información personal. Todas las personas, debidamente identificadas, tienen reconocido el derecho de acceso a las informaciones sobre ellos registradas (art. 35.1 CRP y art. 27 LPDP) con las excepciones de la legislación sobre secretos del Estado y de la Justicia. El ejercicio de este derecho no puede ser limitado, aunque puede someterse a reglas para evitar un ejercicio abusivo (art. 28.1 LPDP). El Convenio 108 del Consejo de Europa exige que las peticiones de acceso se puedan formular a intervalos razonables y sin demora o gastos excesivos (art. 8.b.); en la legislación comparada, por ejemplo, se autoriza al sujeto pasivo a exigir el pago de un canon razonable. La información debe ser comunicada de forma inteligible. Dispone el art. 28.2 LPDP que la información debe ser transmitida en lenguaje claro, exenta de codificaciones y debe corresponder rigurosamente al contenido del registro. En el caso de información médica, el acceso es indirecto, ya que la información debe ser comunicada por medio de un médico designado por la persona interesada (art. 28.3).

c) Los *derechos de rectificación, integración y cancelación*. Consecuencia del ejercicio del derecho de acceso puede ser el de estos derechos para asegurar la calidad de los datos, de la que es uno de sus presupuestos la exactitud y actualidad de los datos.

Así, según el art. 30.1 LPDP, cualquier persona tiene derecho a exigir la corrección de las informaciones inexactas que le afecten (derecho de rectificación) y a que se completen las omitidas total o parcialmente (derecho de integración). La carga de la prueba de la inexactitud corresponde al titular del registro cuando la información hubiera sido proporcionada por él mismo o con su consentimiento o si no hubiere comunicado su alteración (art. 30.2).

La LPDP reconoce, igualmente, el derecho de cancelación expresamente. Cualquier persona tiene derecho a la supresión de las informaciones personales que se tengan en ficheros automatizados y que hayan sido obteni

das por medios ilícitos o engañosos o cuyo registro o conservación no sean permitidos (art. 30.1. *in fine*). En el sistema de la Ley rige el principio de limitación temporal de conservación de los datos: los datos pueden conservarse sólo el tiempo estrictamente necesario para su finalidad. Así, el responsable del fichero está obligado a destruir los datos una vez transcurrido el plazo de conservación autorizado (art. 23), ya que los ficheros se crean por tiempo determinado (*cfr.*, el art. 18.i, que exige que en la solicitud de informe o autorización para crear un fichero automatizado debe figurar el tiempo de conservación de los datos personales). Por otra parte, la destrucción de datos puede ser ordenada por la CNPDPI (art. 8.1.g en relación con los arts. 20 y 23). Una manifestación concreta del derecho de cancelación es el derecho reconocido a cualquier persona para exigir que su nombre y dirección sean eliminados de ficheros de direcciones utilizadas para el *marketing* directo o *mailing* (art. 30.3).

Un aspecto importante del tratamiento automatizado de datos es el referido a su uso. El art. 15 LPDP, a este efecto, dispone que los datos personales sólo pueden ser utilizados para la finalidad determinante de su recogida, salvo autorización concedida por ley. Ya nos hemos referido más arriba al uso de datos en los trabajos de investigación o con fines estadísticos –uso en forma anónima, salvo consentimiento expreso del interesado– (art. 11.2 y 11.4); prohibición de utilizar perfiles de personalidad obtenidos como resultado de un tratamiento automatizado de información como fundamento único de decisiones judiciales, administrativas o disciplinarias (art. 16). También nos hemos referido con cierto detalle a la prohibición y restricciones del tratamiento automatizado de datos personales sensibles (art. 11).

C) Transmisión de datos.

En relación con el uso de los datos personales destaca el tema de la interconexión de *ficheros automatizados*. La regla general es la prohibición de interconectar datos personales (art. 24.1). Excepcionalmente se permite la interconexión de datos públicos –esto es, los que constan en un documento público oficial, exceptuados los elementos confidenciales– entre entidades que persigan los mismos fines específicos (art. 25). La regla general puede ser exceptuada mediante ley, que deberá definir expresamente los tipos de interconexión autorizados y su finalidad (art. 26). En cualquier caso, esta utilización conjunta de ficheros automatizados que contengan datos personales debe ser autorizada preceptivamente por la CNPDPI (art. 8.1.d.).

Una cuestión íntimamente relacionada con la interconexión de ficheros automatizados es la de la atribución de un *número de identificación personal único* [19]. El art. 24.2 LPDP dice literalmente que «no está permitida la atribu-

[19] En España la creación del número de identificación fiscal (NIF) por el art. 113 de la Ley 33/1987, *de 23 de diciembre, de Presupuestos Generales del Estado para 1988, desarrollado por el Real Decreto 338/1990, de 9 de marzo*, ha suscitado la cuestión sobre si es compatible la atribución de un número nacional único a cada persona con el derecho a la autodeterminación

ción de un número ciudadano para interconectar ficheros automatizados de datos personales que contengan informaciones de carácter policial, criminal o médico». *Sensu contrario* cabría atribuir un número de identificación personal para interconectar ficheros automatizados de datos personales que contengan cualesquiera otras informaciones que no fuesen de carácter policial, criminal o médico. Esta interpretación no es correcta ya que la Constitución contiene una prohibición absoluta de atribuir un número de identificación personal único en su art. 35.3: «Queda prohibida la atribución de un número nacional único a los ciudadanos». En otro caso, habría que reputar inconstitucional el art. 24.2 de la Ley por vulnerar el art. 35 de la Norma fundamental.

El problema del *flujo transnacional de datos* es abordado por la LPDP en su art. 33, que concuerda con el art. 12 del Convenio del Consejo de Europa. El intercambio internacional de datos queda sometido al régimen general de la Ley (art. 33.1). Además, se establece el principio de «protección equivalente»: la CNPDPI puede autorizar flujos transfronterizos de datos si el Estado de destino garantiza una protección equivalente a la de la Ley (art. 33.2). Por último, se prohíbe el flujo transnacional si con ello se pretende eludir las prohibiciones o condiciones de la Ley o hacer posible la utilización ilícita de los datos (art. 33.3)[35].

D) Obligaciones del sujeto pasivo.

El conjunto de derechos del sujeto activo del derecho a la autodeterminación informativa vincula a los sujetos pasivos, que están sometidos a obligaciones genéricas y específicas.

Las obligaciones *genéricas* del responsable de los ficheros o soportes informáticos –definido en el art. 2.h.– son la reserva y la garantía de la seguridad de los datos. Los responsables de los ficheros automatizados, así como las personas que, en ejercicio de sus funciones, tengan conocimiento de los datos personales en ellos registrados, están obligados al *sigilo profesional*, durante y al término de sus funciones (art. 32.1), sin que suponga vulneración de este deber de sigilo el proporcionar las informaciones obligatorias de

---

informativa. Para P. LUCAS MURILLO DE LA CUEVA (*El derecho a la autodeterminación informativa*, *cit* pp. 188-192) el NIF por sí sólo no perjudica ni al derecho a la intimidad ni al derecho a la autodeterminación informativa, aunque puede permitir la lesión de los derechos fundamentales, especialmente si se generaliza su uso en las relaciones privadas. Por contra, para S. A. BELLO PARTIDAS, el art. 113 de la Ley 38/1987, entendiendo como habilitación general e ilimitada a la Administración tributaria para que reglamentariamente regule la utilización del NIF en la forma y manera que estime más conveniente, debe ser considerada fundamentalmente inconstitucional. *Vid* El NIF. «Algunas consecuencias de su incardinación en nuestro ordenamiento jurídico» en AA.VV., *Encuentros sobre informática y Derecho 1990-1991*, Universidad Pontificia de Comillas, Madrid, 1992, pp. 159-170.

[35] El flujo transnacional de datos personales es la base sobre la que descansa el Sistema de Información de Schengen (cfr. los arts. 92-119 y 126-130 del Convenio de 1990). En general, sobre el flujo internacional de datos, *vid.* A. E. PÉREZ LUÑO: *Nuevas tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las nuevas tecnologías de la información*, Fundesco, Madrid 1987, pp. 87-90.

acuerdo con las leyes (art. 32.2). La obligación de la *seguridad de los datos* implica que el responsable debe adoptar las cautelas frente al acceso indebido de terceros o alteraciones fortuitas. El art. 21 establece que los ficheros automatizados deben estar equipados con sistemas de seguridad que impidan la consulta, modificación, destrucción o adición de los datos por persona no autorizada a hacerlo y que permitan detectar desvíos de información intencionados o no. Este artículo concuerda con el art. 7 del Convenio del Consejo de Europa.

Las obligaciones *específicas* son las generadas por derechos subjetivos del sujeto activo del derecho a la autodeterminación informativa.

3. Garantías.

A) Garantías institucionales.

El eje de la Ley es la creación de un órgano de control de la aplicación de la Ley, denominado *Comisión Nacional de Protección de Datos Personales Informatizados* (CNPDPI), al que dedica su capítulo II (arts. 4 a 10), además de otros preceptos dispersos en los que se le atribuyen competencias en concreto.

Frente a la opción por un órgano unipersonal (los comisarios alemanes de datos, federal o territoriales, el inspector de datos sueco, el registrador británico) o por un órgano colegiado (la Comisión Nacional de la Informática y de las Libertades francesa), la Ley portuguesa opta por el modelo francés.

La CNPDPI es un órgano colegiado compuesto por siete miembros, de elección inter-poderes: tres (el presidente y dos vocales) son elegidos por la Asamblea; otros dos vocales son magistrados, uno juez elegido por el Consejo Superior de la Magistratura, el otro fiscal elegido por el Consejo Superior del Ministerio Público; y, los dos restantes vocales, han de ser personas de competencia reconocida, designados por el Gobierno (art. 5).

Lo decisivo de la posición de la CNPDPI es su autonomía efectiva frente a los poderes públicos: es una *autoridad administrativa independiente* [21]. Así la califica el art. 4.2: «La CNPDPI es una entidad pública independiente con poderes de autoridad, que funciona junto a la Asamblea de la República y dispone de servicios propios de apoyo técnico y administrativo». La dispo

[21] Sobre la Administración independiente o neutral *vid.* J. M. Sala Arquer: «El Estado neutral. Contribución al estudio de las Administraciones independientes», REDA 42 (1884), pp. 401-422; F. J. Jiménez de Cisneros Cid: *Los organismos autónomos en el Derecho público español: tipología y régimen jurídico*, INAP, Madrid, 1987, pp. 307-340; A. Jiménez-Blanco: *Derecho público del Mercado de Valores*, Centro de Estudios Ramón Areces, Madrid, 1989, pp. 92-107; F. López Ramón: «El Consejo de Seguridad Nuclear: un ejemplo de Administración independiente», RAP 126 (1991), pp. 189-216. En la doctrina francesa C.-A. Colliard y G. Timsit (dir): *Les autorités administratives indépendantes*, PUF, París, 1988, especialmente el estudio del presidente de la CNIL, J. Fauvet: «La Commission nationale de l'informatique et des libertés», pp.146-149.

nibilidad de medios personales y materiales propios para desempeñar su cometido es un aspecto importante para garantizar su autonomía funcional.

La elección o designación de los miembros de la CNPDPI por los poderes legislativo, judicial y ejecutivo es, igualmente una garantía de su independencia. Esta se ve reforzada por la duración de su mandato, cinco años (art. 10.2) que supera la del mandato del Parlamento y del Gobierno (cuatro años, art. 174 CRP).

Ahora bien, lo determinante de su posición independiente es el conjunto de potestades que la Ley le atribuye para cumplir las funciones asignadas. Su competencia genérica es «controlar el procesamiento automatizado de datos personales con riguroso respeto a los derechos humanos y de las libertades y garantías consagrados en la Constitución y en la Ley» (art. 4.1). A la Comisión le corresponde velar por la aplicación del régimen jurídico establecido en la Ley.

La creación y mantenimiento de ficheros, bases o bancos de datos es controlada por la CNPDPI. El régimen de creación de ficheros automatizados se diferencia según contengan datos personales sensibles voluntariamente ofrecidos, o bien, datos personales no sensibles. En el primer caso, debe existir un informe previo de la CNPDPI, tanto si el titular del fichero es un servicio público como si es una entidad privada; en este último supuesto el régimen es de autorización (art. 17.1 en relación con el art. 8.a. y b.). En el segundo caso, es decir, si los ficheros no contienen datos sensibles, la creación debe ser comunicada (art. 17.3).

En la solicitud de informe o autorización, así como en la comunicación dirigida a la CNPDPI, debe declararse la identidad del responsable del fichero; las características del fichero y de su finalidad; los servicios encargados del procesamiento de la información; los datos personales contenidos en el registro; la forma de recogida y actualización de datos; la finalidad a la que se destinan los datos; las entidades a las que pueden ser transmitidos y en qué condiciones; la interconexión de los datos; las medidas de seguridad; el tiempo de conservación de los datos; la categoría de las personas que tienen acceso directo a los datos; la forma y condiciones de ejercicio de los derechos de acceso, rectificación, integración y cancelación (arts. 18 y 19).

El régimen de creación de ficheros fijado por la Ley no es muy claro. En el caso de creación de ficheros de datos personales sensibles se intenta diferenciar dicho régimen según que el responsable del fichero sea una persona pública o privada, ya que se somete a un régimen de informe previo o de autorización, respectivamente. La Ley debería haber creado expresamente un *registro público*, dependiente de la CNPDPI, en el que constase la información sobre los ficheros de bancos existentes, las personas públicas o privadas que los mantienen, siguiendo el modelo de la *Data Lag* sueca de 1973, sometiendo al régimen de autorización e inscripción registral los bancos que

contengan datos sensibles y al de comunicación e inscripción si no son datos sensibles, de modo que la CNPDPI pudiese denegar la inscripción en el registro si el fichero no se somete al régimen legal. El desarrollo reglamentario de la Ley debe completar la garantía institucional mediante la creación del referido registro.

La CNPDPI es titular de potestad reglamentaria. Así, puede emitir directivas para garantizar la seguridad de los datos (art. 8.1.e.); fijar genéricamente las condiciones de acceso a la información, del derecho de rectificación y actualización (art. 8.1.f.). Además, tiene la facultad de proponer su reglamento a la aprobación de la Asamblea (art. 10.3).

La CNPDPI recibe las quejas, reclamaciones y peticiones de los particulares (art. 8.1.h.). Como consecuencia de éstas, puede promover los procedimientos judiciales para interrumpir el procesamiento de datos, impedir el funcionamiento de ficheros y proceder a su destrucción (art. 8.1.g.). Igualmente, debe denunciar al Ministerio Público las infracciones penales (art. 8.1.j.). El desarrollo de estas funciones debe llevar implícita la posibilidad de inspecciones para comprobar si los ficheros comprendidos en el ámbito de aplicación de la Ley se ajustan a su régimen.

La Comisión es un órgano administrativo, y como tal, emite actos administrativos (p. ej., autorizaciones de creación de ficheros, de interconexión de datos) susceptibles de recursos ante el Tribunal Supremo Administrativo (art. 8.2).

Por último, dado que la CNPDPI funciona junto al Parlamento, puede dirigir a la Asamblea sugerencias y recomendaciones relativas al ejercicio de sus competencias. Asimismo, debe dar publicidad a su actividad mediante un informe anual.

B) Delitos y sanciones.

La LPDP tipifica en su capítulo VIII (arts. 34-43) una serie de delitos castigados con penas privativas de libertad[123]. Se tipifica la utilización ilegal de datos (art. 34); la obstrucción al ejercicio de los derechos de acceso, rectificación e integración (art. 35); la interconexión ilegal de ficheros y la atribución de un número de identificación personal (art. 36); el falseamiento de la información de la solicitud de constitución o mantenimiento de ficheros y la omisión de la comunicación de constitución de ficheros que no contengan datos sensibles (art. 38); el acceso ilegal a los datos; la falsificación o destrucción de datos (art. 39); la desobediencia a la orden de interrupción del funcio-

[123] Sobre la protección penal de la libertad informática, *Vid.* P. MORALES PRATS: *La tutela penal de la intimidad: privacy e informática*, Destino, Barcelona, 1984; C. M. ROMEO CASABONA: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información*, Fundesco, Madrid, 1988, pp. 25-34; J. BUIX REIG: «Protección jurídico-penal de la intimidad e informática» en en AA.VV., Congreso sobre Derecho Informático. *Texto de Ponencias y Comunicaciones. Edición previa*, 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 449-492.

namiento de un fichero y la denegación del deber de colaboración (art. 40); y la vinlación del deber de sigilo (art. 41).

Además de las penas privativas de libertad, se puede imponer como pena accesoria la publicidad de la sentencia en los periódicos, a expensas del condenado (art. 43).

La Ley debería haber tipificado, junto a las infracciones penales, infracciones y sanciones administrativas, así como ilícitos civiles y la correspondiente indemnización de daños y perjuicios. Como señala el art. 10 del Convenio 108 del Consejo de Europa, el régimen de recursos y sanciones debe perseguir que los principios básicos del régimen de protección de datos personales sean respetados.