© *Dereito* Vol. 9, n.º 2: 49-81 (2000) • ISSN 1132-9947

UNA NUEVA EXIGENCIA DE LA LIBERTAD: LA PROTECCIÓN DE LOS DATOS PERSONALES "SENSIBLES"

Ana Garriga Domínguez
Universidade de Vigo

I. Introducción.- II. Garantías comunes: principios de calidad de los datos y derechos de los afectados.- III. Garantías específicas. La especial protección de los datos sensibles.- IV. Consideraciones finales.

I. Introducción

Tanto en el ámbito de las Administraciones Públicas, como en el de las entidades privadas de las sociedades desarrolladas, se recaban, almacenan y tratan automatizadamente un gran número de informaciones sobre millones de personas relativas a multitud de facetas de su vida. Estos datos son recogidos con las más diversas finalidades: gestión de clientes, gestión de cobros y pagos, selección de personal, historiales clínicos, tarjetas de crédito, educación, seguros de vida y salud, investigación, etc. En demasiadas ocasiones, basándose exclusivamente en esos datos registrados en ficheros informáticos se adoptarán decisiones relativas a las personas a las que se refieren.

Por otra parte, el conocimiento de tan exhaustiva información permitirá, de un modo relativamente sencillo vigilar a cualquier individuo[1], con lo que podrán verse gravemente afectados su libertad y sus derechos fundamentales.

---

[1] En este sentido, destaca HEREDERO, la preocupación suscitada en torno al uso de las tarjetas de crédito, *"en cuanto que permite registrar el comportamiento de las personas, formar automáticamente perfiles"* y adoptar decisiones sobre ellas sin que sean tenidas en cuenta ni consultadas. En *"La informática y el uso de la información personal"*, en RIBERO, A. M. y SANTODOMINGO, A.: *Introducción a la informática jurídica*, Fundesco, Madrid, 1986, p. 35.

Los tratamientos de datos personales permiten obtener un esquema de la personalidad bastante aproximado. Este conocimiento proporciona la posibilidad de controlar a cualquier individuo, en especial si desconoce qué datos relativos a su vida poseemos, de forma semejante a como lo haríamos si pudiésemos ver a través de las paredes de su casa, le pinchásemos el teléfono y violásemos su correo. Este poder permite obtener una *"radiografía"* de su vida, hasta el punto de que se puede afirmar que el uso de la tecnología informática *"hace posible una vigilancia de hecho de la vida cotidiana del individuo"*[2]. Pues, las nuevas tecnologías de la información permiten el registro de una serie de datos que separadamente carecen de importancia, pero que adecuadamente relacionados permiten obtener el perfil de una persona. De este modo nos encontramos con que *"nuestra vida individual y social corren (...) el riesgo de hallarse sometidas a lo que Frosini ha calificado, con razón, de "juicio universal permanente""*[3].

Además, con frecuencia, muchas de las decisiones relativas a individuos o grupos de personas van a descansar exclusivamente en el uso del perfil informático y ello significará normalmente su discriminación en muchas de las actividades de la vida cotidiana. Ante este hecho nos encontraremos indefensos al desconocer que, quien decide, conoce informaciones que consideramos olvidadas o secretas, o bien que la decisión se basa en el perfil obtenido a través del tratamiento automatizado de datos públicos u obtenidos de fuentes accesibles al público[4], que aisladamente considerados son inofensivos. A este respecto, destaca François RIGAUX[5] que las modernas técnicas de penetración en las aptitudes profesionales o de comportamiento individual se apoyan, hoy, en los métodos informáticos que establecen correlaciones entre determinadas características y comportamientos concretos a los que se les confiere una apariencia de rigor científico. Basándose en estas correlaciones se construye el perfil de una persona cuya utilización, a su juicio, presenta

---

2 Ibidem, p. 34.

3 PÉREZ LUÑO, A. E.: *Vittorio Frosini y los nuevos derechos de la sociedad tecnológica*, en Informatica e Diritto, 1-2, Edizioni Scientifiche Italiane, 1992, p. 104.

4 Si bien puede afirmarse que la información que ha sido revelada deja de ser íntima, puesto que es pública, no es menos cierto que la naturaleza de esa información va a verse sustancialmente modificada por el simple hecho de que pase a formar parte de una base de datos.

5 RIGAUX, F.: *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruxelles, 1990, p. 597 y ss.

una estrecha similitud con el racismo: *se sirve de un perfil consistente en imputar a un individuo ciertas pautas de comportamiento, comunes al grupo en el que le hemos censado y que distinguimos del resto de la población global.* Entonces se establecen normas de conducta y tratamientos diferenciados para los determinados grupos en los que hemos dividido la población[6]. Tales previsiones serán, generalmente, discriminatorias y, sobre todo porque, *"en la creencia de descubrir en el sujeto ciertos signos anunciadores de su comportamiento futuro, el perfil instaura una forma de determinismo incompatible con el atributo más preciado de la libertad, la elección de un futuro autodeterminado"*[7].

Asimismo, la desigualdad sería propiciada por la acumulación informatizada de datos personales en el acceso a los centros de poder y control social.

Los derechos fundamentales en su aspecto o dimensión subjetiva, "*son derechos individuales que tienen al individuo por sujeto activo y al Estado por sujeto pasivo*"[8] y cumplen una función de garantía a los ciudadanos de "*un status jurídico o la libertad en un ámbito de existencia*"[9]. En este sentido se habla de dimensión subjetiva de los derechos fundamentales. Pero, a la vez, los derechos fundamentales "*son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto esta se configura como marco de una convivencia humana justa y pacífica*"[10], plasmada primero en el Estado de Derecho y más tarde en el Estado social y democrático de Derecho. Es decir, en su dimensión objetiva, los derechos fundamentales actúan como elementos esenciales para establecer el necesario equilibrio entre poderes en las sociedades democráticas.

Esta función exige, que en las relaciones entre el Estado y la sociedad o entre los miembros de ésta, *"no se den situaciones de marcada desigualdad*

---

6 Piénsense, por ejemplo, en un individuo al que hemos situado en un grupo de posibles delincuentes, a un recluta al que se le sitúa como probable protagonista de actos de insubordinación o en un posible grupo de alumnos conflictivos de un colegio, a los que se somete a una vigilancia y a una inspección particular o a un individuo al que, simplemente, hemos situado entre los que no tienen determinadas actitudes o ideologías, negándole el acceso a un determinado puesto de trabajo o cargo público.

7 RIGAUX, F.: *La protection de la vie privée et des autres biens de la personalité*, ob. cit, p. 598.

8 STC 64/1988, fundamento jurídico 1º. Esta es la tesis clásica de los derechos civiles y políticos.

9 STC 25/1981, fundamento jurídico 5º.

10 Ibidem.

en el acceso al poder que implique para determinadas personas o grupos humanos una marginación de la libertad"[11]. Cuando unos pocos controlan los grandes bancos de información gozan de una gran ventaja sobre aquellos que no pueden llegar a ella, lo que, a la postre va a suponer un más fácil acceso al poder de los primeros en detrimento de los segundos, objeto de vigilancia y control. Ha de tenerse en cuenta, además, que en las modernas sociedades, *"la capacidad de actuación política se haya íntimamente ligada al acceso y control de la información"*[12], por lo que el equilibrio socio-político hace necesario que se garantice a los grupos sociales la participación en condiciones de igualdad de las informaciones registradas en los bancos de datos. Con esta nueva tecnología de la información se ha propiciado *"una nueva diferencia en la sociedad humana entre los que pueden participar y los que no pueden participar de la revolución informática"*[13].

El tratamiento automatizado de las informaciones personales ha supuesto un cambio sustancial en los instrumentos de garantía de la vida privada y de la libertad. Las posibilidades infinitas de almacenamiento, organización, cruce de datos, la disponibilidad a larga distancia y, más recientemente, el acceso mundial a los mismos a través de *"internet"*, ha obligado al reconocimiento de nuevos derechos a las personas y el establecimiento de una normativa específica de protección de datos personales. En este camino hacia el establecimiento de garantías merece un lugar destacado, junto con la paulatina aprobación de leyes de protección de datos, la sentencia de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán, en la que se perfila, por primera vez, el derecho a la autodeterminación informativa o libertad informática.

---

[11] PÉREZ LUÑO, A. E.: *"Los derechos humanos en la sociedad tecnológica"*, en LOSANO, M. Y OTROS: *Libertad informática y leyes de protección de datos*, Centro de Estudios Constitucionales, Madrid, 1990, p. 138.
Para este autor, en este momento, la agresión a la igualdad se produce de manera más virulenta que en ningún otro período histórico, «*desde el momento en que se desarrolla una profunda disparidad entre quienes posean, o tienen acceso, al poder informático y quienes se hallan marginados de su disfrute*». En PÉREZ LUÑO, A. E.: *Del Habeas Corpus al Habeas Data*, Informática y Derecho, número 1, UNED, Centro Regional de Extremadura, Mérida, 1992, p. 156.

[12] PÉREZ LUÑO, A.E.: *Derechos humanos, Estado de Derecho y Constitución*, quinta edición, Tecnos, Madrid, 1995, p. 338.

[13] FROSINI, V.: *Informática y Derecho*, trad. Jorge Guerrero y Marino Ayerra Redín, Temis, Bogotá, 1988, p. 34.

El Tribunal Constitucional Alemán configura a partir del derecho general de la personalidad garantizado en la Ley fundamental de Bonn[14], *"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"*[15]. El Tribunal extrae del derecho al libre desarrollo de la personalidad la facultad de cada individuo de disponer sobre la revelación y el uso de sus datos. Y entiende el derecho a la autodeterminación informativa como la facultad general de disponer de los datos propios. A juicio de DENNINGER, el Tribunal alemán ha puesto el acento de forma decisiva en la cuestión más importante, al entender que *"la autodeterminación informativa no sólo depende de los datos sino de su elaboración"*[16]. Es decir, el peligro para el derecho a la autodeterminación de las personas no se encuentra en el carácter del dato, más o menos íntimo; tampoco importa que el dato tenga, o no, carácter secreto, *"lo que importa es su utilidad y la posibilidad de su aplicación"*[17]. Por tanto, la necesidad de proteger mediante los adecuados instrumentos jurídicos los datos relativos a las personas, no depende tanto de sí pertenecen o no a su ámbito íntimo, *"cuanto a las posibilidades de elaboración e interrelación propias de la tecnología informática"*[18]. El riesgo, por tanto, para las libertades depende de unas posibilidades de interrelación prácticamente ilimitadas. Pues como destaca TRAVERSI, la nota peculiar de cualquier sistema de elaboración electrónica es que permite la memorización de un número elevadísimo de información de cualquier tipo, seleccionarla, agregarle otra o confrontarla con la contenida en otro banco y transmitirla a cualquiera y todo esto en tiempo real y sin límite de espacio ni fronteras[19]. Así, un dato carente de interés aisladamente considerado, bajo las condiciones de la elaboración automática de datos, puede adquirir un nuevo valor de referencia, por lo que ya no existe, *"ninguno sin interés"*[20]. Lo

---

14 Destaca PÉREZ LUÑO, que para el Tribunal Constitucional germano *"el principio básico del ordenamiento jurídico establecido por la Grundgesetz es el valor y la dignidad de la persona que actúa como libre autodeterminación al formar parte de una sociedad libre"*. En *Nuevas tecnologías, Sociedad y Derecho*, Fundesco, Madrid, 1987, p. 127.

15 Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán, *Boletín de Jurisprudencia Constitucional*, nº 33, p. 126, trad. de Mariano Daranas.

16 DENNINGER, E.: *El derecho a la autodeterminación informativa*, en PÉREZ LUÑO, A.E.: *Problemas actuales de documentación y la informática jurídica*, Tecnos Madrid, 1987, p. 273.

17 Ibídem.

18 Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983.

19 TRAVERSI, A.: *Il Diritto dell'informatica*, Seconda edizione, Ipsoa Informática, 1990, p. 92.

20 Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán.

importante es *"la finalidad con la cual se reclaman los datos y que posibilidades de interconexión y de utilización existen"*[21]; y, sólo cuando estén claros estos puntos *"se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa"*[22].

Sin embargo y dentro de su línea de ponderación de los bienes, destaca PÉREZ LUÑO, *"el Tribunal Constitucional de Karlsruhe advierte que el derecho a la autodeterminación informativa no carece de límites."*[23]. El ciudadano de un Estado social de Derecho no tiene un poder absoluto e ilimitado sobre sus datos personales, al ser una persona que se desenvuelve en una comunidad social en la que la información y la comunicación resultan imprescindibles. *"De ahí, que la información, aún aquella que se refiere a datos personales, ofrece una imagen de la realidad social que no puede ser patrimonio exclusivo del interesado."*[24]

El derecho a la autodeterminación informativa se fija especialmente en la utilización que se haga de las informaciones resultantes de interrelacionar determinados datos personales y del perfil que se obtenga. Es decir, no se trata de impedir a terceros el acceso a determinadas informaciones privadas, sino que, lo que este derecho pretende evitar, es determinados usos de esas informaciones y del resultado de su tratamiento. Por esta razón, lo que está en juego no es propiamente la intimidad de las personas, sino su propia identidad. Las consideraciones anteriores nos llevan, con Vittorio FROSINI, a afirmar que *"la libertad informativa representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del rigth of privacy, (...) consiste, también, en la "libertad de informarse", es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia "identidad informática""*[25].

Evidentemente, las posibles agresiones a la intimidad de las personas, a su libertad o al ejercicio de sus derechos fundamentales se van a ver

---

21 Ibídem.

22 Ibídem.

23 PÉREZ LUÑO, A.E.: *La defensa del ciudadano y la protección de sus datos*, en *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, p. 59.

24 Ibídem.

25 FROSINI, V.: Informática y Derecho, ob. cit., p. 23.

agravadas cuando los datos recogidos y tratados automatizadamente pertenezcan a la categoría de los denominados "datos sensibles". Las informaciones sensibles son aquellas que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana. Son los datos relativos a la ideología, religión o creencias, origen racial, salud, vida sexual y, también, los relativos a la comisión de infracciones administrativas o penales.

Pudiera pensarse que, dada la naturaleza tan especial de este tipo de datos, se encontrarían registrados en contadas ocasiones. Sin embargo, la realidad muestra que esto no es así. En nuestro país existen, según informaciones facilitadas por la propia Agencia de Protección de Datos, numerosos ficheros que contienen este tipo de información. Hasta la fecha de 30 de abril de 2000, existían en España los siguientes ficheros de datos sensibles, inscritos en el Registro General de Protección de Datos[26]:

	TITULARIDAD PÚBLICA	**TITULARIDAD PRIVADA**
DATOS ESPECIALMENTE PROTEGIDOS	62	368
Ideología	*39*	*167*
Creencias	18	40
Religión	13	189
OTROS DATOS ESPECIALMENTE PROTEGIDOS	2.059	3.822
Origen racial	*85*	*60*
Salud	1.840	3.803
Vida sexual	352	113
DATOS RELATIVOS A INFRACCIONES	1.235	0
Infracciones Penales	*727*	*0*
Infracciones Administrativas	842	0

[26] El Registro de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros de datos personales, a fin de garantizar que los titulares de los datos, puedan ejercer los derechos de información,

El total de los ficheros que contienen datos personales sensibles 7.546 suponen, sin duda, un pequeño porcentaje en relación con el total de los ficheros de datos personales inscritos en el Registro General de Protección de Datos: 241.985, de los cuales 30.576 son de titularidad pública y los restantes 211.409 son privados[27]. No obstante, por la particular naturaleza de estos datos personales, por lo íntimo de las informaciones a las que hacen referencia, así como por lo particularmente graves que pueden ser las consecuencias de su utilización fraudulenta para las personas a las que se refieren, ha propiciado que en todas las regulaciones, tanto nacionales como internacionales, hayan gozado de una especial posición traducida en un reforzamiento de las medidas adoptadas para su garantía y protección.

II. Garantías comunes: principios de calidad de los datos y derechos de los afectados

Los datos sensibles, por su especial naturaleza, gozan de una particular protección, más rigurosa que el resto de los datos personales. Esas garantías específicas serán abordadas en la tercera parte de este trabajo.

En este momento y siguiendo la lógica de la Ley Orgánica 15/1999, de Protección de Datos Personales analizaré los principios que deben respetarse en la recogida y tratamiento de cualesquiera datos personales, así como los derechos de los titulares de esos datos. Principios y derechos forman los elementos del denominado derecho a la autodeterminación informativa o libertad informática.

---

acceso, rectificación y cancelación. Deben inscribirse en el Registro los siguientes ficheros, actos y documentos: a) Los ficheros automatizados de datos personales de los que sean titulares la Administración General del Estado, las entidades y organismos de la Seguridad Social; los organismos autónomos del Estado, las sociedades estatales y entes del sector público, las Administraciones de las Comunidades autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes y las entidades que integran la Administración; b) Los ficheros de datos personales de los que sean titulares las personas privadas, físicas o jurídicas; c) Las autorizaciones para la transmisión internacional de datos personales cuando sea preceptiva la autorización del Director, es decir, cuando el país de destino no cuente con un nivel de protección equiparable al español; d) Los códigos tipo.

27 Todos estos datos que se aportan corresponden a los ficheros inscritos a fecha de 30 de abril de 2000, por lo que la actualidad el número de ficheros inscritos ha podido incrementarse.

La Ley Orgánica 15/1999, como hizo la LORTAD[28] en su momento, desarrolla el mandato contenido en el artículo 18.4 de la Constitución según el cual *"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"*. Con este precepto, nuestra Norma Fundamental ha incorporado una nueva garantía constitucional en respuesta a las nuevas amenazas que las modernas tecnologías de la información suponen para la dignidad, la libertad y los derechos de las personas. Esta garantía se caracteriza por constituir un derecho fundamental autónomo a controlar las informaciones que nos conciernen y que en muchas ocasiones realiza una función instrumental en orden a proteger y garantizar el ejercicio de otros derechos del mismo rango[29].

Decir que estamos ante un derecho fundamental autónomo significa afirmar que se trata de un derecho distinto del derecho a la intimidad y que, aunque está estrechamente relacionado con ella, tiene un contenido específico distinto del derecho a la intimidad. El derecho a la autodeterminación informativa o libertad informática es según afirma el propio Tribunal Constitucional *"el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de las personas"*[30] provenientes del uso torticero del tratamiento informático de datos personales.

Por otra parte como acabamos de apuntar, el derecho a la autodeterminación informativa realiza frecuentemente una función de garantía de otros derechos fundamentales. De acuerdo con el artículo constitucional del que arranca en nuestro Ordenamiento la normativa sobre protección de datos, las limitaciones que el contenido del derecho a la autodeterminación informativa impone al tratamiento automatizado de datos personales –lo que el artículo 18.4 denomina *"la informática"*– tienen la finalidad de garantizar el pleno ejercicio de los derechos. El texto constitucional menciona expresamente dos

---

28 Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

29 De hecho el Tribunal Constitucional y así lo ha venido estableciendo de forma reiterada desde 1993, ha venido caracterizando el derecho a la autodeterminación informativa o libertad informática como un derecho instrumental ordenado a la garantía de otros derechos y un derecho fundamental autónomo con un contenido específico. Entre otras, SSTC 254/1993, de 20 de julio; 60/1998, de 16 de marzo, 105/1998, de 19 de junio y 202/1999, de 8 de noviembre.

30 STC 254/1993, de 20 de julio.

de los derechos que podrían verse amenazados por un uso abusivo e ilegítimo de las nuevas tecnologías de la información: los derechos al honor y a la intimidad. Sin embargo, otros como la libertad sindical, el derecho a la huelga, la libertad ideológica o religiosa, el derecho a no ser discriminado o el derecho a acceder en condiciones de igualdad a la función pública, por ejemplo, podrían resultar igualmente amenazados[31].

Podemos distinguir dos elementos en el contenido mínimo del derecho a la autodeterminación informativa o libertad informática[32]. De un lado un elemento negativo que responde al enunciado literal del art. 18.4 de *limitar el uso de la informática.* De otro, un elemento positivo de control sobre los propios datos[33]. El contenido propio del elemento negativo estaría formado por lo que se conocen como principios de calidad de los datos[34] mientras que el

---

31 Un ejemplo clarificador de cómo el derecho a la autodeterminación informativa realiza esa función instrumental de garante de otros derechos fundamentales lo encontramos en la cuestión resuelta por STC 11/1998, de 11 de enero. El Tribunal Constitucional estimó el amparo interpuesto por un trabajador de RENFE contra la sentencia de la sala de los Social del TSJ de Madrid, que absolvió a la empresa de su conducta de descuento de retribuciones al trabajador por entender que había participado en una huelga, basándose exclusivamente en el dato de afiliación sindical que poseía. El trabajador había proporcionado dicho dato a efectos de retención de la cuota sindical y éste se encontraba registrado en un fichero automatizado. El demandante de amparo pretendió que había sido conculcado su derecho a la libertad sindical y así lo confirmó el Tribunal Constitucional. Cuando el trabajador proporcionó a la empresa la información sobre su afiliación sindical, lo hizo con la exclusiva finalidad de que la empresa, de acuerdo con lo establecido en el art. 11.2 de la Ley Orgánica de Libertad Sindical, descontara de la retribución la cuota sindical y la transfiriera al sindicato. Sin embargo, RENFE, en una decisión unilateral que supuso un trato discriminatorio para el trabajador y con base exclusiva en la clave informática de ese dato, descontó la retribución correspondiente al tiempo que duró la huelga, a pesar de que el trabajador no participó en ella. Este trato peyorativo al trabajador por razón de su adhesión a un sindicato vulnera el contenido esencial de la libertad sindical que el artículo 28.1 de la Constitución consagra como derecho fundamental. Ahora bien, la libertad sindical no fue el único derecho afectado por la decisión empresarial, sino que propio derecho a la autodeterminación informativa resultó, también, directamente conculcado. No obstante, lo que ahora interesa destacar, es que a través de la protección de la persona frente al tratamiento automatizado de sus datos, a través de la protección constitucional a los datos personales íntimos o no, se están garantizando otros derechos y libertades que pueden resultar afectadas por el uso ilegítimo de esas informaciones.

32 Vid. mi trabajo *"La nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, ¿Un cambio de filosofía?;* en Anales de la Cátedra Francisco Suárez, nº. 34, Universidad de Granada, 2000, p. 299-321.

33 STC 254/1993, de 20 de julio.

34 Principios que establecen todas las leyes de protección de datos con cierta uniformidad, especialmente en el ámbito europeo a partir del Convenio 108 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.

positivo lo formarían los derechos del titular de los datos, recogidos en los Títulos II y III de la Ley Orgánica 15/1999.

a) Elemento negativo: La calidad de los datos

Para el análisis del elemento negativo del derecho a la autodeterminación informativa, debe partirse de la idea básica de que lo que requiere la efectiva tutela de los derechos de los ciudadanos en este ámbito no es la prohibición del uso de la informática, sino su límite. Así, en la medida en que se afecten datos personales, debe someterse a la informática *"a una serie de cautelas y de límites* (que conjuren los riesgos que se derivan de esta actividad, y que) *permitan reparar los daños que origine y evitar que se vuelvan a producir."*[35] Se trata de intentar *"conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información"*[36].

Los límites necesarios para garantizar ambos bienes, los que responden a la necesidad del tratamiento de informaciones personales[37] y los derechos de los ciudadanos, se concretan en exigencias específicas relativas a la recogida, registro y uso de los datos personales y están encaminadas a garantizar tanto la veracidad de la información contenida en los datos, como la congruencia y racionalidad de su utilización. Estos límites, tradicionalmente denominados *"principios de calidad de los datos"*, son los siguientes:

1.- *Principio de pertinencia.* Recogido en el artículo 4.1 de la Ley, significa que los datos personales deben estar relacionados con el fin perseguido por lo que deberán de ser adecuados y no excesivos en relación con las finalidades para las que se hayan registrado. Ha de garantizarse, una *"clara conexión entre la información que se recaba (...) y el objetivo para el que se solicitó"*[38]. Es decir, no podrán solicitarse ni registrarse más datos que los estrictamente necesarios para llevar a cabo la investigación de que se trate o cumplir la finalidad legítima. Por lo tanto, no podrán recabarse más datos

---

35 MURILLO DE LA CUEVA, P.L.: *Informática y protección de datos personales*, Cuadernos y Debates nº 43, Tecnos, Madrid, 1993, p. 39.

36 Exposición de Motivos del Convenio 108 del Consejo de Europa.

37 Por ejemplo intereses comerciales de empresas, por necesidades de gestión, de eficaz funcionamiento de las Administraciones Públicas, de persecución del fraude fiscal y a la Seguridad Social, etc.

38 MURILLO DE LA CUEVA, P.L.: Informática y protección de datos personales, ob. cit., p. 65.

que aquellos que sean estrictamente necesarios en ese momento, aunque fuesen susceptibles de serlo para cumplir los objetivos futuros.

2.- *Principio de finalidad.*[39] Establecido en al artículo 4.1 y 2, se encuentra íntimamente conectado con el anterior y supone que sólo se podrán recoger y tratar automáticamente los datos personales que sean adecuados a las finalidades legítimas para las que se hayan obtenido y, también, que los datos personales no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos. Es decir, los datos sólo podrán recogerse e informatizarse de acuerdo con una finalidad legítima y determinada y por lo tanto no podrán recogerse datos para finalidades contrarias a las leyes o al orden público, debiendo ser respetuosas con los valores constitucionales y los derechos fundamentales. Tampoco se recabarán datos personales para el cumplimiento de objetivos imprecisos o inconcretos y, en último término, los datos "*no se utilizarán de forma incompatible con dichas finalidades*"[40].

La nueva redacción del principio de finalidad del artículo 4.2 de la Ley Orgánica 15/1999 introduce un cambio respecto de la legislación anterior. En lugar de prohibir el uso de los datos personales para finalidades "*distintas*" de aquellas para las que los datos hubieran sido recogidos como hacía la LORTAD, lo prohíbe para finalidades "*incompatibles*". ¿Debe entenderse entonces que es posible el uso de los datos para finalidades distintas cuando sean compatibles con aquéllas para las cuales se recogieron los datos? ¿Cuáles serían entonces las finalidades compatibles?

El cambio en la forma de expresar el principio de finalidad es fruto de la evolución legislativa en las distintas generaciones de leyes de protección de datos. La redacción de la LORTAD era semejante a la de leyes como la francesa o la luxemburguesa de 1978 y 1979, respectivamente. Fue el Convenio 108 del Consejo de Europa el que, por primera vez, alteró la concepción del principio de finalidad al establecer en su artículo 5.b) que los datos se registrarán para unas finalidades determinadas y legítimas "*y no se*

---

[39] Este principio es denominado también "*principio de utilización no abusiva*". En DEL PESO NAVARRO, M. y RAMOS GONZÁLEZ, M. A.: *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*, Díaz de Santos, Madrid, 1994, p. 94.

[40] PÉREZ LUÑO, A. E.: *Los derechos humanos en la sociedad tecnológica*, ob. cit., p. 168.

utilizarán de forma incompatible con dichas finalidades".[41] También la redacción de la Directiva 95/46/CE, objeto de transposición en la Ley 15/1999, emplea una expresión semejante. En el artículo 6.1.b) se establece que los datos deben registrarse para unos fines determinados, explícitos y legítimos y no serán *"posteriormente tratados de forma incompatible con dichos fines".*

El nuevo texto del artículo 4 acoge, por tanto, la redacción de la Directiva. De acuerdo con la exigencia de que la finalidad de la recogida de los datos sea legítima, explícita y determinada, ésta deberá definirse de la forma más precisa posible y el uso que sea haga de esos datos con posterioridad, deberá ser compatible con la finalidad de la recogida de los mismos. Expresamente sólo se establece que serán compatibles los tratamientos posteriores con fines históricos, estadísticos o científicos, al igual que hace la norma comunitaria. En el considerando 29 de ésta se aclara además, que los fines anteriores no se considerarán incompatibles en la medida en que se establezcan las garantías adecuadas para impedir que los datos sean utilizados para tomar medidas o decisiones contra cualquier persona. En mi opinión, en este mismo sentido debe interpretarse el artículo 4 de la Ley 15/1999, ya que de lo contrario se vaciaría de contenido el principio de finalidad.

Este principio significa, además, que una vez utilizados para la finalidad legal para la que hubiesen sido recabados no podrán ser reutilizados para el cumplimiento de objetivos distintos a aquéllos para los que se solicitaron y registraron. Cumplida la finalidad legítima que autorizó su recogida y tratamiento los datos personales habrán de ser cancelados, no pudiendo conservarse, durante más tiempo que el necesario para el cumplimiento de esos fines, en forma que permita la identificación del interesado (art. 4.5 de la Ley de Protección de Datos).

3.- *Principio de veracidad y de exactitud.* El punto tercero del artículo 4, exige que los datos sean exactos y estén actualizados de forma que respondan con veracidad a la situación del afectado. Los datos no deberán responder a una situación anterior a la de la recogida de los mismos y en este momento inexistente y, además, deben ser veraces, es decir, deberá

---

[41] Vid. HEREDERO HIGUERAS, M.: *La Directiva comunitaria de protección de datos de carácter personal*, Aranzadi, Pamplona, 1997, en especial pgs. 103 a 105.

existir una perfecta correspondencia *"entre el discurso que marcan los hechos y el que se trasmite al receptor de la información"*[42].

Si por alguna razón los datos personales no respondieran con veracidad a la situación del afectado, al resultar inexactos o incompletos, la ley exige su cancelación o su sustitución de oficio por los correspondientes datos rectificados o completados.

4.- *Principio de lealtad.* Los datos personales deberán recabarse sin engaños o falsedades por parte de quien los solicita, prohibiéndose su recogida *"por medios fraudulentos desleales o ilícitos"*[43] .

5.- *Principio de seguridad de los datos.* El artículo 9 de la Ley exige al responsable del fichero o al encargado de su tratamiento que adopten las medidas necesarias para garantizar la seguridad de los datos personales evitando su alteración, pérdida, tratamiento o acceso no autorizados. El actual desarrollo legislativo del principio de seguridad prohíbe, asimismo, el registro de datos personales en ficheros que no reúnan las condiciones que han sido determinadas por el *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal,* aprobado por Real Decreto 994/1999, de 11 de junio.

La importancia de este principio, en orden a garantizar los derechos de los afectados, ha crecido en los últimos tiempos. Al mismo tiempo que se ha producido un espectacular desarrollo de las capacidades de proceso de los ordenadores, en la microelectrónica y en el software, lo que ha permitido la proliferación de sistemas informáticos potentes y fáciles de utilizar, se han incrementado *"los riesgos que amenazan a los datos almacenados y procesados por ellos y, en consecuencia, a los ciudadanos a quienes dichos datos conciernen"*[44], pues mayores son los medios para *atravesar* las barreras de seguridad de un fichero. Por ello, las medidas de seguridad deben mejorarse y adecuarse a estos avances.

---

42 ESPINAR VICENTE, J. M.: *La primacía del derecho a la información sobre la intimidad y el honor;* en GARCÍA SAN MIGUEL, L. Y OTROS: *Estudios sobre el derecho a la intimidad,* Tecnos, madrid, 1992, p.65.

43 Artículo 4.7 de la Ley Orgánica 15/1999.

44 CUEVA CALABIA, J. L.: *La LORTAD y la seguridad de los sistemas automatizados de datos personales;* en *Actualidad Informática Aranzadi,* nº 13, octubre, Aranzadi, 1994, p.7.

b) El elemento positivo: Los derechos de los afectados

Es el derecho a controlar los propios datos. Este control se lleva a cabo a través de determinadas facultades[45], que formarían el contenido del llamado *habeas data* o *habeas scriptum.*

El *habeas data* surge en el seno de la última generación de derechos humanos como "*un cauce procesal para salvaguardar la libertad de la persona en la esfera informática*".[46] De forma paralela a como el *habeas corpus* pretende garantizar la libertad física del individuo, el *habeas data* aparece como "*la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados*"[47], frente a los nuevos fenómenos abusivos que limitan la esfera informática de la libertad de la persona.

El conjunto de facultades que forman parte del elemento positivo del derecho a la autodeterminación informativa o libertad informática son los siguientes:

1.- *El derecho del titular de los datos a que se le informe* de los bancos de datos existentes, de su titularidad y finalidad.[48] El derecho a la información del artículo 5 de la Ley garantiza que las personas de las que se soliciten datos personales, sean informadas de manera previa a la recogida de los mismos, de modo expreso, preciso e inequívoco a cerca de las siguientes cuestiones:

---

45 La Exposición de Motivos de nuestra primera Ley de Protección de Datos, la L.O. 5/1992, de 29 de octubre, los configuraba jurídicamente *"como derechos subjetivos encaminados a hacer operativos los principios genéricos (...) otorgándoles virtualidad normativa y eficacia jurídica (...), principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático".*

46 PÉREZ LUÑO, A. E.: *Intimidad y protección de datos personales: del habeas corpus al habeas data*; en GARCÍA SAN MIGUEL Y OTROS: *Estudios sobre el derecho a la intimidad*, ob. cit., p. 40.

47 PÉREZ LUÑO, A.E.: *Del habeas corpus al habeas data;* en *Informática y Derecho*, nº 1, UNED, centro regional de Extremadura, Mérida, 1992.

48 El derecho de información de las personas respecto del tratamiento automatizado de sus datos de carácter personal se configura en la Ley en una doble vertiente. Por un lado, la se garantiza al afectado el derecho a ser informado en el momento de la recogida de sus datos de los aspectos relativos a su tratamiento informático y, de otra parte, se establece que cualquier persona pueda conocer, *"recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, su finalidad y la identidad del responsable del fichero»* (artículo 14 de la L. O. 15/1999).

- De la existencia de un fichero o tratamiento de datos personales, de la finalidad de su recogida y de los destinatarios de éstos.
- De si es obligatorio o facultativa la respuesta a las preguntas planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a facilitarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o de su representante.

Al igual que ocurría con el principio de finalidad, se ha producido un avance positivo en la regulación de este derecho. Siguiendo la pauta marcada por la Directiva 95/46/CE, se establece la obligatoriedad de informar a los interesados cuando los datos no hayan sido recabados directamente de ellos. No obstante, esta obligación no tiene un carácter absoluto, sino que la ley regula varias excepciones. Así no será necesario informar al interesado:

a) Cuando expresamente una ley lo prevea;

b) Cuando el tratamiento tenga fines históricos, estadísticos o científicos;

c) Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o

d) Finalmente, cuando los datos procedan de fuentes accesibles al público y se destinen a las actividades de publicidad o prospección comercial.

Las dos últimas excepciones merecen, a mi juicio, que nos detengamos un momento en su análisis.

Por lo que respecta a aquellos casos en los que resulte imposible o sea extremadamente difícil cumplir con la obligación de información, corresponderá a la Agencia de Protección de Datos o al organismo autonómico correspondiente, en función del número de afectados, la antigüedad de los datos y a las posibles medidas compensatorias, determinar cuando nos encontramos ante uno u otro caso. Es decir, será la Agencia de Protección de Datos a quien competa establecer el nivel exigencia del cumplimiento de este derecho, que en todo caso deberá ser riguroso a fin de garantizar los derechos fundamentales de los ciudadanos.

Especialmente interesante es la última excepción ya que afecta directamente a los datos obtenidos de fuentes accesibles al público. Es realmente digno de mención el cambio operado en la regulación de este tipo de datos. La legislación anterior no contemplaba la necesidad de comunicar al afectado que determinados datos contenidos en las denominadas fuentes accesibles al público[49], habían sido recogidos e iban a ser elaborados automatizadamente con una concreta finalidad. Expresamente se excluía la necesidad de solicitar su consentimiento siempre que los datos tuvieran esta procedencia. En la práctica esto suponía que estos datos se iban a utilizar, por un lado, no sólo sin el consentimiento del interesado, sino también sin su conocimiento y, por otro, para finalidades diferentes para las cuales los había facilitado y que justificaban su publicidad.

Ahora, aún cuando entre las excepciones al consentimiento del afectado siga figurando la de que los datos se recojan de fuentes accesibles al público, en los términos que luego veremos, el interesado deberá ser informado de la recogida de sus datos y de la finalidad y destinatarios del tratamiento, entre otras cuestiones. Esta obligación va a suponer una nueva consideración por parte del responsable del fichero en el momento de captar los datos, puesto que incluso cuando se obtengan de este tipo de fuentes será *"necesario proporcionar información al interesado de su inclusión en un fichero"*[50] y aún en el supuesto en que no sea obligatorio el consentimiento del afectado. La más importante consecuencia de todo ello es, en mi opinión, que, además de tener conocimiento de la *circulación* de sus datos, el interesado podrá ejercitar, puesto que conoce que están contenidos en un fichero automatizado, ya que ha debido ser informado también de este aspecto, los derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la Ley.

Hay una excepción, no obstante, al derecho de información en relación con los datos obtenidos de fuentes accesibles al público: *cuando sean destinados a actividades de publicidad y prospección comercial.* Sin embargo,

---

[49] Además, ahora se establecen cuales son estas fuentes accesibles al público en el artículo 3.j) y se regulan específicamente en el artículo 28.

[50] GARCÍA BEATO, M. J.: *Principios y derechos en la Ley 5/1992, de 29 de octubre y en la Directiva 95/46/CE*; en *Jornadas sobre el Derecho español de la protección de datos personales*, Agencia de Protección de Datos, Madrid, 1996.

en este caso, más que hablar de excepción deberíamos de hacerlo de un retraso en la comunicación de la información. Pues de acuerdo con el artículo 30 de la Ley, cuando los datos procedan de estas fuentes, en cada comunicación que las empresas de publicidad y marketing directo hagan al interesado deberán informarle del origen de los datos, de la identidad del responsable del fichero, así como de los derechos que le asisten. Por tanto esta excepción solamente supone postergar el ejercicio del derecho de información al momento en que se produzca la primera comunicación, lo que no es óbice para considerar que lo ideal es que la información se produjera en el momento de la recogida de los datos, si bien, en todo caso, la regulación actual es notablemente mejor que la anterior, por lo que a la garantía de los derechos de los afectados se refiere.

2.- *Derecho del afectado a que se solicite su consentimiento* para la recogida, tratamiento y cesión de sus datos personales. Este derecho está estrechamente relacionado con el anterior, ya que es condición indispensable para que el interesado pueda prestar el consentimiento para el tratamiento de sus datos, el cumplimiento previo del contenido del derecho de información. Antes de prestar su consentimiento ha de conocer las consecuencias que se derivarán del mismo, así como las características y la naturaleza del fichero, etc. Esto supone que quien recaba esta información personal deberá informar al afectado, previa, expresa, precisa e inequívocamente, de las consecuencias de su consentimiento para que, de esta forma, "*pueda ejercer su derecho a la autodeterminación informativa con pleno conocimiento del alcance de sus actos*"[51]. Es decir, el derecho de información entendido como requisito previo a la recogida de datos personales, posibilita determinar al titular de los mismos el nivel de protección y reserva que desea para ellos y, por tanto, prestar su consentimiento de forma "*consciente e informada*"[52].

Las dudas que suscitaba la anterior regulación del consentimiento del afectado, a cerca de la posibilidad de admisión del consentimiento implícito o tácito, parecen quedar desde ahora resultas. La adaptación a la directiva a supuesto también en este aspecto una mejoría notable. No es que la anterior regulación admitiese cualquier consentimiento. No, el consentimiento debía

---

[51] MURILLO DE LA CUEVA, P. L.: *Informática y protección de datos personales, ob. cit., p. 56.*

[52] OROZCO PARDO, G.: *Los derechos de las personas en la LORTAD;* en *Informática y Derecho, nº 6-7,* UNED, Centro Regional de Extremadura, Mérida, 1994, p. 177

prestarse *"en unas condiciones específicas y para unas finalidades concretas"*[53], sin embargo ahora ya no existe la menor duda de cuáles son las condiciones y las características de éste. El consentimiento se configura como toda manifestación de la voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales. Además, el consentimiento deberá prestarse de forma inequívoca, es decir, desaparece la posibilidad de consentir tácitamente el tratamiento de los datos personales, en el sentido de que no existe manifestación directa pero se han proporcionado voluntariamente informaciones sin estar obligados jurídicamente a ello. En la Ley 15/1995, el consentimiento se presta de manera voluntaria e inequívoca o no se presta, es decir, *"o se exige el consentimiento explícito o se exime de todo tipo de consentimiento"*[54].

El aspecto negativo en la actual regulación del consentimiento lo encontramos en la larga lista de excepciones al mismo, más larga aún que en la LORTAD, si bien no todas las excepciones merecen la misma valoración. No entraré a valorarlas todas, respecto de las dos primeras excepciones al consentimiento del afectado contempladas en el artículo 6.2, las que lo excluyen cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias y en aquellos casos en los que se refieran a las partes en un contrato me remito a lo escrito en otro lugar[55].

La tercera excepción prevista hace referencia a los supuestos en los que los datos tengan como finalidad proteger un interés vital del interesado en el supuesto de que esté física o jurídicamente incapacitado para prestar su consentimiento. Parece claro que la excepción, si bien no se especifica, se refiere a los datos relativos a la salud. Ésta se encuentra plenamente justificada por el bien jurídico que se pretende proteger, la vida o la salud del interesado o de terceras personas, se trata de proteger un interés esencial. Por otra parte, debe entenderse que, sólo cuando el interesado esté física o jurídicamente incapacitado, podrá prescindirse de su consentimiento de

---

53 MURILLO DE LA CUEVA, P. L.: *Informática y protección de datos personales*, ob. cit., p. 56.

54 FREIXES SANJUAN, T.: *Obtención y utilización de datos personales automatizados*; en *Jornadas sobre el Derecho español de la protección de datos personales*, Agencia de Protección de Datos, Madrid, 1996, p. 124.

55 Vid. mi trabajo *La protección de los datos personales en el Derecho español*, Universidad Carlos III - Dykinson, Madrid, 1999, p. 206 y ss.

acuerdo con el artículo 6.2 en relación con el 7.6, ambos de la Ley Orgánica15/1999.

Finalmente se exceptúa también el consentimiento de afectado en la recogida de datos personales cuando *"éstos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"* (art. 6.2, último inciso).

A diferencia de la LORTAD que exceptuaba en todo caso el consentimiento del afectado cuando los datos se recogieran de fuentes accesibles al público, la actual regulación introduce dos requisitos:

a) Que su tratamiento sea necesario para la satisfacción del interés legítimo de quien recoja o a quien se cedan los datos. La anterior regulación ya exigía que las finalidades de la recogida, tratamiento y uso de los datos personales fueran legítimas. Así pues, debemos entender que, cuando se hace referencia al interés legítimo del responsable del tratamiento o de un tercero se está haciendo referencia a una cuestión distinta. Estamos ante el problema de *"interés prevalente"*[56]. La Directiva comunitaria no aclara los supuestos posibles de prevalencia de otros intereses sobre el interés del titular de los datos. El considerando 30 no los enumera sino que deja a criterio de los Estados miembros la determinación de las condiciones en los que pueden recogerse, usarse y cederse los datos personales *"en el desempeño de actividades legítimas de gestión ordinaria"*.

Está claro que el juego de los intereses se refieren al ámbito privado, ya que los intereses de las Administraciones Públicas, priman con carácter general sobre los de los particulares al exceptuarse su consentimiento en las condiciones del artículo 6 de la Ley. Por otra parte, al no establecerse una determinación más concreta de cual debe ser el interés prevalente podría llegarse a la conclusión de que los intereses del mercado priman sobre los del interesado[57]. Así por ejemplo prevalecería el interés legítimo, sin duda, del

---

[56] Sobre la evolución legislativa de la cuestión del interés prevalente vid. HEREDERO HIGUERAS, M.: *La Directiva comunitaria de protección de datos de carácter personal*, ob. cit, p. 112 y ss.

[57] Así lo entiende HEREDERO en la Directiva 95/46/CE, por cuanto el artículo 7.f) remite expresamente al 1.1, ambos de la norma comunitaria, que sienta el principio de libre circulación de datos como norma. Ibidem, p. 113.

control de la morosidad o de evaluación de solvencia patrimonial[58] o el interés de las empresas de publicidad o marketing directo, también legítimo. La minoración de los efectos perjudiciales para el afectado, al menos en el primer caso, vendría por la obligación de informarle de que sus datos han sido recogidos y van a ser usados con esas finalidades, de acuerdo con el contenido del derecho de información, según acabamos de ver y, también, en la medida en que debe respetarse el segundo de los requisitos.

b) Que no se vulneren los derechos fundamentales del titular de los datos. Con la expresa mención de este límite se está haciendo referencia claramente a la función instrumental que el derecho a la autodeterminación informativa desempeña en relación con las libertades públicas y los demás derechos fundamentales. Este limite se podría concretar de la forma que sigue: no podrá prescindirse del consentimiento del afectado, aún cuando existan otros intereses legítimos en juego, si ello supone un vaciamiento tal del contenido esencial del derecho a la autodeterminación informativa que impida su función protectora de otros derechos fundamentales y éstos pudieran ser afectados. Parece claro que los derechos fundamentales de las personas deben prevalecer, en todo caso, frente a los intereses del mercado u otros intereses legítimos[59].

---

58 Interpretación que corrobora el artículo 29 de la Ley que establece que "*quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto...*"

59 Este fue, por ejemplo, el caso resuelto por STC 202/1999, de 8 de noviembre. El Tribunal Constitucional entendió que las facultades empresariales de control del absentismo laboral, aunque era un interés legítimo amparado por la legislación laboral vigente, no podían prevalecer sobre los derechos fundamentales a la intimidad y a la libertad informática de los trabajadores. La cuestión que suscitó la demanda de amparo fue la recogida y almacenamiento de datos relativos a la salud de los trabajadores de una empresa bancaria con la finalidad probada, según el Tribunal Constitucional, de ejercer las facultades empresariales de control del absentismo laboral. Para ello se creó un fichero informático en el que figuraban, entre otros datos personales, las altas y bajas médicas y los diagnósticos médicos que motivaban dichas bajas laborales. Todos esos datos se recogían y almacenaban sin el consentimiento de los trabajadores, lo que motivó que el Alto Tribunal considerase que la medida empresarial, "*sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad*", no superaba el juicio de proporcionalidad para la consecución de la finalidad perseguida. Pues, no se trataba de una medida "*de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad*".

2.-*Los derechos de acceso, rectificación y cancelación.* El derecho de acceso de los afectados a las informaciones que les conciernen, junto con *los derechos de rectificación y cancelación* de datos erróneos o inexactos, constituye el instrumento idóneo para que el ciudadano pueda controlar la información que sobre él tienen registrada entidades públicas y privadas. De la misma manera que los derechos de información y a prestar o no el propio consentimiento suponen instrumentos a *priori* de control sobre los datos personales, anteriores al momento en que estos pasan a formar parte de un fichero informatizado; los derechos de acceso, cancelación y rectificación lo son a *posteriori*, en el sentido de que estos derechos permiten ejercer el control sobre aquellos datos que han sido recabados y registrados en el pasado.

Estamos ante tres derechos, recogidos en los artículo 15 y 16 de la Ley, que garantizan la facultad del afectado de acceder a sus propios datos registrados en un fichero informático, el derecho a que los datos que figuren de manera inexacta y errónea en un fichero automatizado sean corregidos e integrados y la facultad de eliminar del fichero automatizado aquellos datos de carácter personal *"que no deban figura en él, ya sea por que nunca debieron ser registrados, ya sea porque habiéndose recogido legalmente, diversas causas exigen su supresión"*[60].

3.- *El derecho al olvido*, según el cual ciertas informaciones deben ser eliminadas pasado un determinado período de tiempo. Por una parte, es un instrumento necesario para el efectivo cumplimiento del principio de finalidad, en el sentido que supone que los datos recogidos y registrados sólo podrán usarse de acuerdo con una finalidad concreta, lo que implica la cancelación de los que ya no sean necesarios para la realización de la misma. Por otra, supone este derecho que ciertas informaciones, pasado un cierto período de tiempo, deben ser eliminadas. Los datos personales no van a poder ser conservados, salvo en el caso en que se decida su mantenimiento por valores históricos, científicos o estadísticos, cuando hayan dejado de ser útiles para la función prevista, con las excepciones previstas en la legislación específica prevista al efecto (obligaciones fiscales, seguros, etc.).

El derecho al olvido tiene por objeto contrarrestar uno de los riesgos más característicos del procesamiento informático de la información relativa

---

[60] MURILLO DE LA CUEVA, P.L.: *Informática y protección de datos personales*, ob. cit., p. 79.

a una persona: la posibilidad de recuperar en un instante cualquier dato por insignificante que éste parezca, aún habiendo transcurrido decenas de años, lo que implica la desaparición de la garantía que suponía para la intimidad de las personas la fragilidad de la memoria humana.

4.- *El derecho de oposición.* Es una de las novedades de la nueva Ley de Protección de Datos.[61]

Su importancia reside en que *"se configura como un instrumento garante de carácter netamente preventivo o cautelar"*[62] frente a las soluciones típicas de remedio *a posteriori,* propias del sistema judicial.

La Ley reconoce al interesado el derecho a oponerse al tratamiento de sus datos personales en aquellos casos en los que no sea necesario su consentimiento, siempre que una ley no disponga lo contrario y existan motivos fundados y legítimos relativos a una concreta situación personal. En estos casos el responsable del tratamiento deberá excluir los datos relativos al interesado.

El derecho de oposición tiene su razón de ser en cuanto instrumento de defensa que impida el vaciamiento legal del derecho a la autodeterminación informativa en los casos en los que la Ley establece criterios de legitimación para el tratamiento de datos personales distintos de la voluntad o el interés del afectado, ya que *"se limita un derecho fundamental de la persona por entrar en juego otros derechos jurídicamente protegidos"*[63]. Por ello, para GARCÍA BEATO, *"la existencia de razones legítimas y la situación particular justifican el derecho de oposición de cualquier ciudadano y ello porque el principal objetivo de la Ley en cualquier caso ha de ser la protección de los principios"*[64] reconocidos en la Constitución.

---

61 Aunque existía ya en la LORTAD recogido en el artículo 29, respecto de los datos recogidos para fines de publicidad y de marketing directo. La regulación de este particular derecho de oposición se encuentra recogida en el artículo 30.4 de la Ley 15/1999, en idénticos términos.

62 CORRIPIO GIL-DELGADO, R.: *Las nociones de interés público e interés legítimo en relación al ejercicio del derecho de oposición del interesado*; en *Jornadas sobre el Derecho Español de la Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, p. 287.

63 Ibídem, p. 293.

64 GARCÍA BEATO, M. J.: Principios y derechos en la Ley Orgánica 5/1992, de 29 de octubre y en la Directiva 46/95/CE, ob. cit., p. 49.

Debe apuntarse, no obstante, que para evaluar el alcance real del derecho de oposición, así como sus posibilidades de ejercicio por parte de los ciudadanos, deberemos esperar a su desarrollo reglamentario al que remite el artículo 17 de la Ley de Protección de Datos Personales sobre *procedimiento de oposición, acceso, rectificación y cancelación.*

5.- Impugnación de valoraciones.

El artículo 13 de la nueva Ley de Protección de Datos, ha incluido novedades en la regulación relativa a la impugnación de las decisiones basadas exclusivamente en el perfil. Esta disposición, trata de contrarrestar los efectos perjudiciales que pueden derivarse para un individuo, en sus relaciones públicas o privadas, de la reconstrucción artificial de su perfil personal, en base al tratamiento automatizado de sus datos y en numerosas ocasiones simplemente, en base a datos estadísticos relativos al grupo social al que pertenece. Además, la conclusión a la que se llegue a través de dicho tratamiento puede no corresponderse con la realidad.

No obstante, como ocurría en la LORTAD no se prohíbe realizar tales tratamientos, conservarlos o transmitirlos, simplemente se prohíbe una de las múltiples aplicaciones que tendrá el perfil informático de una persona. No se impide, sin embargo que estos sean utilizados, por ejemplo, con fines comerciales o de marketing directo[65].

Ahora bien, y esta es la novedad, a diferencia de la regulación anterior que simplemente establecía el derecho del afectado a impugnar las decisiones, públicas o privadas, basadas exclusivamente en el perfil personal, se recoge un nuevo derecho: *el derecho del afectado a no verse sometido a una decisión con efectos jurídicos o que le afecte de manera significativa*, con el único apoyo en los resultados de un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

Sin embargo y pese a que se enuncie este nuevo derecho, parece que la Ley es pesimista y presume que no se va a respetar, ya que seguidamente, en los mismos términos de la legislación anterior, establece el derecho a

---

[65] De hecho es habitual, en la actualidad, que las técnicas de investigación de mercados se basen en gran medida en el estudio del <<*perfil del consumidor*>>.
Sobre esta cuestión vid. GRANDE ESTEBAN, I. y ABASCAL FERNÁNDEZ, E.: *Fundamentos y técnicas de investigación comercial*, ESIC Editorial, Madrid, 1994.

impugnar las decisiones privadas o los actos administrativos basados exclusivamente en la valoración de su comportamiento con único fundamento en el perfil informático. Es decir, si bien el afectado tiene derecho a no verse sometido a decisiones que le afecten con ese único fundamento, como es notorio que ello se produce, la ley le concede también el derecho a impugnarlas. Para facilitarle la impugnación se regula también el deber del responsable del fichero de informarle sobre los criterios de valoración y el programa utilizado en el tratamiento, imagino que con la finalidad de el afectado pueda argumentar en contra de la fiabilidad de este último.

De la lectura del nuevo artículo 13, al menos esta es mi percepción, se deduce el escepticismo del legislador en cuanto a que se vaya a respetar el primero de los derechos mencionados en este precepto, por eso se recoge también el segundo. Esta postura responde a una visión realista de la situación y eso es positivo. Sin embargo y por eso la lectura de este artículo es tan poco alentadora, va a ser prácticamente imposible probar que *"la decisión"* se haya basado exclusivamente en el perfil de la personalidad. Pues como respecto de la LORTAD escribía LUCAS MURILLO, "*una cosa es reconocer un derecho del afectado a la impugnación* (o como en la regulación actual a que no se le someta a esa decisión) *y considerar viciados el acto administrativo o una decisión privada adoptados en su perjuicio con el único fundamento de una valoración sobre su persona y, otra, bien distinta, es demostrarlo*"[66].

III. Garantías específicas. La especial protección de los datos sensibles

Son varias las cautelas que contiene la Ley Orgánica 15/1999 en relación con la información personal sensible. Al igual que en la LORTAD, se distinguen tres grupos o categorías de datos que, por diversas razones exigen una protección máxima, habida cuenta de lo directamente comprometidas que se hallarían la dignidad y libertad por su uso ilegítimo. Además, las decisiones a las que sirvan de base, podrán suponer, en ocasiones, una violación del principio de igualdad de algún otro derecho fundamental.

1. El primer grupo de datos sensibles estaría integrado por las informaciones que revelen la ideología, afiliación sindical, religión y creencias.

---

[66] MURILLO DE LA CUEVA, P.L.: *Informática y protección de datos personales*, ob. cit., p. 83.

El reforzamiento de la protección a este tipo de datos que establece la ley consiste en dos exigencias:

a) Sólo podrán ser objeto de tratamiento cuando el afectado preste su consentimiento de forma expresa y por escrito.

b) Cuando se proceda a recabar el consentimiento del interesado, deberá advertírsele de su derecho a no prestarlo.

La protección especial a tan delicada información consiste en reforzar los derechos de información y consentimiento del interesado. Los requisitos anteriores no serán necesarios cuando los datos relativos a ideología, creencias, religión o afiliación sindical tengan como destino los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical y se trate de datos relativos a sus afiliados, asociados o miembros. El consentimiento, en estos casos, sólo será necesario en caso de cesión de los datos.

En este punto y aunque pudiera parecer paradójico, es muy positiva la novedosa excepción a la especial reglamentación de los datos personales relativos a la ideología, afiliación sindical o creencias. Lo positivo, evidentemente, no es que se exceptúe el requisito del consentimiento expreso y por escrito del interesado para tratar este tipo de datos. Los positivo es que los ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y otras entidades sin ánimo de lucro con finalidades análogas están sometidos al régimen general de la Ley y no expresamente excluidos como en la legislación anterior.

La LORTAD limitaba la aplicación de sus disposiciones, a los ficheros de los partidos políticos, sindicatos e iglesias respecto de los datos referentes a sus asociados, a los supuestos de cesión de los datos. Al excluir del ámbito de aplicación de la LORTAD a este grupo de ficheros, se impedía al afectado que ejercitase los derechos establecidos en la misma, vedándole la oportunidad de acceder, rectificar o cancelar esa información. Es decir, en definitiva se dejaba fuera de su control sus datos, en tanto estuviesen en poder de esas instituciones.

La situación actual es muy diferente, por varias razones. En primer lugar, es importante destacar la ubicación de su regulación. Se encuentra en

el artículo 7 de la Ley que regula los datos especialmente protegidos, los *datos más sensibles*. En segundo lugar, están sometidos al régimen general de protección de la Ley 15/1999 y al especial del artículo 7. Es decir, con la excepción de que no será necesario el consentimiento expreso y por escrito del afectado, se le aplicará la regulación general relativa a la calidad de los datos y a los derechos de los afectados, así como la prohibición específica para los datos sensibles de crear ficheros para almacenar exclusivamente esta categoría de datos. Por tanto, ahora se garantiza el contenido mínimo del derecho a la autodeterminación informativa también en relación con esos ficheros concretos, a diferencia de la reglamentación anterior que significaba de hecho que quien se afiliase a un sindicato, militase en un partido político o confesase una determinada religión, renunciaba al ejercicio de un derecho fundamental. Además, por cuanto el derecho a la autodeterminación informativa actúa también como un derecho instrumental, tanto la libertad sindical, como la libertad ideológica y el pluralismo político que nuestra Constitución consagra como un valor superior de nuestro Ordenamiento, así como la libertad religiosa, alcanzarán unas mayores cuotas de desarrollo, ya que se garantiza una mayor autodeterminación y libertad para las personas que deciden integrarse estas instituciones.

2. Un segundo grupo de informaciones sensibles lo forman los datos relativos al origen racial, a la salud y a la vida sexual. Estos datos no podrán ser recogidos, tratados o cedidos salvo que el interesado consienta expresamente o cuando, por razones de interés general, lo disponga una ley.

La tercera garantía específica para los datos sensibles, regulada en el artículo 7.4 de la Ley, consiste en la prohibición de crear ficheros con la exclusiva finalidad de almacenar datos personales relativos a la ideología, religión, creencias, afiliación sindical, origen racial o étnico o vida sexual. Por lo tanto, esta tercera cautela pretende reforzar la protección de los dos grupos anteriores de datos sensibles, a excepción de loa informaciones referentes a la salud.

También se establece en relación con los dos grupos de informaciones sensibles, recogidas en los apartados 2 y 3 del artículo 7, que podrán ser objeto de tratamiento cuando resulte necesario *"para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de*

datos se realice por un profesional sanitario sujeto a secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto". Igualmente, en los casos en los que el tratamiento de datos sea necesario para salvaguardar el interés vital del afectado o de otra persona y éste se encuentre física o jurídicamente incapacitado para prestar su consentimiento.

Se trata de una excepción, como ya adelanté al tratar la exigencia del consentimiento del afectado, a mi juicio, plenamente justificada por el bien jurídico que se pretende proteger: la vida o la salud del interesado o de terceras personas. Sin embargo, parece un poco excesivo que la excepción se haga para todas las categorías de datos incluidas en los apartados 2 y 3 del artículo 7. Pues, si bien esa excepción parece lógica y razonable respecto de los datos relativos a la salud o tal vez también para los referentes a la vida sexual, no se me ocurre que relación puede existir entre otras categorías, como por ejemplo la ideología o la afiliación sindical, y el interés vital del afectado o de terceros o con el tratamiento o diagnóstico médicos.

3. Los datos sensibles relativos a la salud reciben un tratamiento legal diferente habida cuenta de su propia naturaleza. Son datos relativos a la salud cualquier información concerniente a la salud pasada, presente y futura, física o mental de un individuo. Es indiferente que se trate de una persona de buena o mala salud o, incluso, un fallecido. Igualmente se encuentran incluidas en esta categoría las informaciones relativas al abuso de alcohol o al consumo de drogas[67].

Se encuentran regulados en el artículo octavo de la Ley, que autoriza a las instituciones y centros sanitarios, públicos y privados, y a los profesionales correspondientes a tratar de forma automatizada los datos relativos a la salud de las personas que acudan a ellos o hayan de ser tratados en los mismos. En estos casos se procederá de acuerdo con lo previsto en la legislación sanitaria.

Nos encontramos ante una situación en la que, claramente, el interés particular debe ceder ante el general más digno de protección, primando la salud de la población sobre los derechos de los particulares. Por tanto, estamos ante un supuesto típico que encajaría perfectamente en la excepción prevista en el apartado 3 del artículo 7 de la Ley.

---

[67] Vid. Memoria explicativa del Convenio 108 del Consejo de Europa, punto 45.

No obstante, es importante insistir en que el artículo 8 sólo autoriza el tratamiento de datos sobre la salud a centros e instituciones sanitarias, en los demás casos deberá estarse a lo previsto en el artículo anterior.

Por otra parte, aún en este caso deberán hacerse algunas precisiones. La Ley General de sanidad garantiza los derechos de los afectados al respeto de su personalidad, dignidad, e intimidad y a la confidencialidad de toda la información relacionada con su proceso y estancia en instituciones sanitarias, públicas o privadas (art. 10 de la Ley General de Sanidad). Es decir, la utilización de los ficheros de datos personales relativos a la salud deberá responder al principio *"de asegurara que la utilización de los datos médicos se hace no solamente con el fin de suministrar a los individuos los mejores cuidados y servicios médicos, sino también, de tal forma que se respeten la dignidad e integridad física y mental de los mismos"*[68].

Igualmente debe insistirse en la idea de que los datos relativos a la salud, como ocurre con las restantes categorías de datos sensibles, se encuentran amparados por el principio de finalidad con lo que no podrán ser utilizados para usos distintos de los estrictamente sanitarios; esto es, para prevenir, controlar y tratar las enfermedades o epidemias, realizar investigaciones, etc.[69]

4. El último grupo de datos personales sensibles incluidos entre los especialmente protegidos en la Ley está integrado por aquellos que hacen referencia a la comisión de infracciones penales o administrativas. Estos datos

---

[68] BUQUICCHIO, M.: *"Informática y libertad: Balance de quince años de actividad en el seno del Consejo de Europa"*, en *Jornadas Internacionales sobre Informática y Administración Pública*, Instituto Vasco de Administración Pública, Oñati, 1986, p.102.

[69] En este línea, la *Recomendación R (81) 1*, adoptada el 23 de enero de 1981 por el Comité de Ministros del Consejo de Europa, relativa a la reglamentación aplicable a los bancos automatizados de datos médicos, entiende que la utilización de los datos relativos a la salud debe limitarse, en principio al personal médico y paramédico para el cumplimiento de las funciones que le son propias y en la medida de sus necesidades. No obstante, en la Recomendación se contempla la posibilidad de su uso para otros fines como son investigación, estadísticas, publicación o enseñanza, siempre que no sea posible identificar al titular de los datos.
En sentido semejante, la Directiva 95/46/CE establece en su artículo 8.3 que no será el consentimiento del afectado para el tratamiento de los datos relativos a la salud cuando resulte necesario hacerlo *"para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento sea realizado por un profesional sanitario sujeto al secreto profesional"*.

sólo podrán figurar en los ficheros de las Administraciones Públicas competentes en los supuestos previstos en sus normas reguladoras. Esta exigencia, es decir, que la posibilidad de crear y mantener ficheros con esta clase de datos se limite en exclusiva a las Administraciones Públicas competentes no sólo responde al objetivo de garantizar la libertad informática del individuo, sino que está también relacionada con *"el objetivo de no frustrar los efectos regeneradores que atribuye a las sanciones el artículo 25 de la Constitución"*[70].

IV. Consideraciones finales

Resulta evidente que ante las agresiones, a la libertad y derechos de los ciudadanos, provinientes del tratamiento automatizado de los datos personales, ya no son suficientes las garantías tradicionales. La esfera de la libertad individual no se protege adecuadamente a través del poder de exclusión del conocimiento de los demás de una parte de nuestra propia vida. El derecho a la intimidad, en su configuración tradicional de libertad negativa, no sirve para asegurarnos en nuestra libertad y derechos. Por ello, las normas sobre protección de datos personales, a través del establecimiento de mecanismos específicos, pretenden garantizar un nuevo ámbito de la libertad: la libertad informática.

Bajo la anterior denominación, el también llamado derecho a la autodeterminación informativa, se configura como una nueva garantía fundamental que, mediante el establecimiento de determinados límites al tratamiento informatizado de informaciones personales y asegurando una serie de facultades a las personas afectadas por tales tratamientos, garantiza su libertad, dignidad y el pleno ejercicio de los demás derechos fundamentales.

Se han analizado las garantías, comunes y específicas, que nuestra normativa establece para proteger aquellas informaciones especialmente delicadas o sensibles en orden a asegurar los anteriores bienes. Sin embargo, sólo se ha hecho referencia a los aspectos positivos de nuestra reglamentación. Por ello, creo necesario y aunque sea de una manera muy breve, hacer mención de otros aspectos que considero criticables, pues, en algún caso, limitan en exceso aquellas garantías.

---

[70] MURILLO DE LA CUEVA, P. L.: *Informática y protección de datos personales*, ob. cit., p. 72.

Respecto de nuestra legislación anterior ya se plantearon críticas y cautelas desde la doctrina científica. Entre las "*sombras*" de la LORTAD[71] destacaban dos de manera especial: la gran cantidad de exenciones a su régimen general y la más aún si cabe numerosa lista de excepciones a los derechos de los afectados. Respecto de la primera cuestión, que no ha sido abordada en este trabajo, debe decirse que las exclusiones del ámbito de aplicación de la nueva Ley son menos numerosas y más razonables y consiguientemente merece una valoración positiva. No así en el caso del segundo aspecto mencionado. La Ley 15/1999 reproduce de forma prácticamente idéntica las constantes excepciones, que limitan el alcance real de los derechos de los interesados[72]. Se reproducen de forma prácticamente igual, en algún caso se introducen variaciones que en nada alteran el sentido del precepto, el contenido de los artículos 18 y siguientes de la LORTAD o el artículo 6 de la misma Ley, al que ya me he referido, tan criticados en su momento por la doctrina[73] y, que en determinados supuestos, dejan prácticamente sin contenido los derechos de los afectados. Tan numerosas excepciones, así como la proliferación de conceptos indeterminados, de nuevo reproducidos, complica bastante la efectiva protección del afectado. Esto sucede, como en la LORTAD, muy especialmente con aquellos ficheros cuya titularidad corresponde a las Administraciones Públicas, en cuyo caso, en aras de unos intereses generales no siempre demasiado claros en la Ley, se vacían prácticamente de su contenido esencial los derechos de los interesados.

Es razonable reconocer que ha habido avances importantes en aspectos determinados, especialmente por lo que se refiere al derecho de información,

---

71 Vid. PÉREZ LUÑO, A.E.: *Manual de Informática y Derecho*, ob. cit., p. 61 y ss.

72 En algún caso incluso incrementa el número de excepciones. Por ejemplo, respecto del consentimiento del afectado en caso de cesión de datos a terceros no sólo se mantienen las del anterior artículo 11, sino que vía disposición adicional se añade alguna más. Es el caso de la disposición adicional sexta que modifica el artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados que establece la posibilidad de que las Entidades Aseguradoras mantengan ficheros comunes con los datos personales de sus asegurados con la finalidad de permitir la tarificación y selección de riesgos. Asimismo se excluye el consentimiento del afectado para la cesión de datos personales a dichos ficheros, aunque esta cesión deba comunicarse al interesado.

73 Alguno de los cuales, como es conocido, habían sido objeto de recurso de inconstitucionalidad por el Defensor del Pueblo, el Parlamento de Cataluña y por el Grupo Parlamentario Popular. Recientemente, el Defensor del Pueblo a interpuesto nuevamente recurso de inconstitucionalidad contra determinados preceptos de la Ley 15/1999, de 13 de diciembre, que reproducen los ya recurridos en 1993 (B.O.E. de 8 de marzo de 2000).

la inclusión bajo el régimen de aplicación de la Ley de los ficheros de datos personales que poseen sobre sus afiliados, los sindicatos, partidos políticos o confesiones religiosas, así como por las novedades vistas en la regulación de los datos personales obtenidos de fuentes accesibles al público. Sin embargo, una consideración general del conjunto de la Ley no merece, en mi opinión, una valoración positiva. Siguen existiendo demasiadas *"y significativas excepciones"*[74] que afectan también, en algunos casos, a los datos sensibles y que impiden que efectivamente se pueda cumplir la misión de garantizar la dignidad y la libertad de las personas en las nuevas sociedades de la información. De hecho, algunas de esas excepciones más bien parece, al igual que sucedía en la LORTAD, que responden a la finalidad contraria, a la de establecer un preciso y eficaz control sobre los ciudadanos.

Igualmente, se hecha en falta que la Ley Orgánica 15/1999 no haya incluido entre los datos especialmente protegidos el número nacional de identificación (D.N.I.) como, sin embargo, recoge la Directiva 95/46/CE en el apartado séptimo del artículo 8. La Directiva incluye entre las normas relativas a categorías de datos personales especiales, el número de identificación nacional o cualquier otro de carácter general, como por ejemplo el Número de Identificación Fiscal (N.I.F.) en nuestro país. La norma comunitaria eleva al máximo las garantías para la protección de este tipo de datos personales aunque no prohíbe la adjudicación de un único número identificador a cada ciudadano, cuya implantación *"constituiría una "llave de acceso" a todos los ficheros"*[75].

A diferencia de otras legislaciones de nuestro ámbito[76], las normas españolas sobre protección de datos personales no prohíben la asignación del un único código identificador a cada ciudadano. Con ello se posibilita la interrelación de todos los datos existentes relativos a una misma persona en los diferentes ficheros, tanto públicos como privados, y la obtención de una forma fácil del perfil o radiografía de la vida de cualquiera, a los que hicimos alusión al inicio de este trabajo. Bajo esas condiciones, resultará muy sencillo hacer un seguimiento exhaustivo de cualquier persona con el consiguiente menoscabo de su libertad y derechos.

---

74 Ibídem, p.62.

75 ROBERT, J.: *Droits de l'homme et libertés fondamentales*, Montchrestien, Cinquième édition, Paris, 1994, p. 380.

76 Por ejemplo, la Constitución portuguesa de 1976.

El Tribunal Constitucional tuvo ocasión de manifestarse acerca de la constitucionalidad del NIF o número de identificación fiscal en sentencia 143/1994, de 9 de mayo, entendiendo que su implantación no violaba el contenido esencial del derecho a la intimidad, con lo que en cierta medida se ha constitucionalizado la atribución del un único código identificador. Por ello y dada la regulación de la Directiva, tenía que haberse aprovechado la aprobación de la nueva Ley de Protección de Datos, sino para impedir la asignación del código único de identificación, al menos para dotar a éste de las máximas garantías incluyéndolo entre la categoría de los datos personales sensibles. Con este olvido, en mi opinión, se dificulta en gran medida el ejercicio del derecho a controlar las informaciones que nos conciernen.

Finalmente y en otro orden de cosas, me gustaría llamar la atención sobre una problemática diferente y me atrevería a afirmar que independiente, de las regulaciones legales sobre protección de datos: el interés comercial de los datos personales. No puede ocultarse que cuando los operadores de mercado no pueden acceder legalmente a los datos personales, incluidos los sensibles, los compran de forma ilegal. Todos los países de nuestro entorno han sufrido esta práctica[77].

Este problema se ha visto incrementado con el fenómeno Internet que posibilita la obtención, legal o ilegal, de datos personales desde cualquier parte del mundo. Por ello y puesto que una normativa internacional *"global"* parece inviable, sería necesario, como se viene reclamando desde los distintos sectores involucrados, que todas las partes implicadas se comprometiesen a respetar unos principios y recomendaciones mínimas que conduzcan a la creación de un código de conducta mundial.

Como se dijo en la introducción, la protección de los datos personales, ni aún la de las informaciones más sensibles, tiene por objeto asegurar simplemente "esos datos", sino que su finalidad última es la de proteger a la persona frente a los abusos de su utilización. Pues, cuando hablamos de garantizar su uso no abusivo, estamos hablando de garantizar la libertad de la persona.

---

[77] Son conocidos los casos en los que ha tenido que intervenir la Agencia de Protección de Datos en relación a cesiones ilegales del censo electoral, filtraciones de los datos de los afiliados a algún partido político, la venta de datos personales desde las oficinas del INEM en determinadas provincias, etc.