

LA NUEVA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES, ¿UN CAMBIO DE FILOSOFÍA?

Ana GARRIGA DOMÍNGUEZ
Universidad de Vigo (España).

RESUMEN

En las sociedades modernas, un gran número de las decisiones que nos afectan descansan en los datos registrados en ficheros informatizados que contienen informaciones sobre millones de personas relativas a un amplio número de facetas de su vida. Para garantizar la dignidad, libertad y el pleno ejercicio de los derechos fundamentales frente al uso torticero de las nuevas tecnologías de la información, el artículo 18.4 de nuestra Constitución ha establecido una nueva garantía constitucional denominada tradicionalmente autodeterminación informativa. Este nuevo derecho es configurado por nuestro Tribunal Constitucional como un derecho fundamental autónomo aunque estrechamente ligado al derecho a la intimidad y un derecho instrumental de garantía de otros derechos fundamentales. El contenido de este derecho es desarrollado en la nueva Ley de Protección de Datos Personales, la Ley Orgánica 15/1999, de 13 de diciembre, que sin duda aporta interesantes y positivas novedades. Sin embargo, al igual que sucedía en el caso de la L.O. 5/1992 LORTAD, siguen existiendo demasiadas sombras que pueden afectar al contenido esencial del derecho a la autodeterminación informativa y que impiden que efectivamente éste pueda cumplir su misión de garantizar la dignidad y la libertad de las personas en las nuevas sociedades de la información.

SUMMARY

In present-day society, a great number of decisions affecting us come from facts recorded in computer files containing information on millions of people relating to a vast number of items in our lives. To guarantee dignity, freedom and full exercise of all our rights against the malicious use of new information technologies, article 18.4 of the Spanish Constitution establishes a constitutional guarantee, namely, information self-determination. This new right is configured by the Constitutional Court as an autonomic fundamental right, although linked to privacy and an instrumental right of guarantee of other fundamental rights. The content of this right is developed in the new "personal data law" (L.O. 15/1999) which contributes positive novelty. Nevertheless, as in L.O. 5/1992, LORTAD, there are too many black points remaining concerning this new right, which prevents the new law from achieving its mission of guaranteeing the dignity and freedom of people in the new information society.

I. INTRODUCCIÓN

En las sociedades modernas un gran número de las decisiones que afectan a las personas, tanto en el ámbito de las Administraciones Públicas como en el de las entidades privadas, descansan en los datos registrados en ficheros informatizados. Estos ficheros contienen informaciones sobre millones de personas relativas a un amplio número de facetas de su vida: trabajo, salud, nivel económico, expedientes académicos, números de teléfonos a los que llama, viajes que realiza, hoteles en los que duerme, productos que adquiere, accidentes de tráfico que haya podido sufrir o, incluso, las películas que alquila en un videoclub¹.

Resulta evidente que a través del conocimiento de tan exhaustiva información resultaría sencillo vigilar a cualquier individuo, con lo que quedaría gravemente afectada su libertad y el ejercicio de sus derechos. No es necesario controlar físicamente a una persona para limitarla o privarla de libertad. Si conocemos un gran número de datos acerca de un determinado individuo y los relacionamos entre sí debidamente, podemos obtener un esquema de su personalidad bastante aproximado. Este conocimiento nos proporciona la posibilidad de controlarlo, especialmente 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 nos permite obtener una *radiografía* de su vida, así como prever sus reacciones y comportamientos. El uso de la tecnología informática “hace posible una vigilancia de hecho de la vida cotidiana del individuo”², al permitir 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.

Por otro lado debe destacarse cómo el uso, exclusivamente, del perfil informático en la toma de decisiones que afecten a una persona 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 que aisladamente considerados son inofensivos. A este respecto, destaca François Rigaux⁴ que

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.

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

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 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 población⁵. 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”⁶.

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, “son derechos individuales que tienen al individuo por sujeto activo y al Estado por sujeto pasivo”⁷ y, además, garantizan a los ciudadanos “un status jurídico o la libertad en un ámbito de existencia”⁸. En este sentido se habla de dimensión subjetiva de los derechos fundamentales. “Pero, al propio tiempo son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica”⁹, 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 requiere que en las relaciones entre el Estado y la sociedad o entre los miembros de ésta, “no se den situaciones de marcada desigualdad en el acceso al poder que implique para determinadas personas o grupos humanos una marginación de la libertad”¹⁰. Cuando unos pocos controlan los grandes bancos de

5. Piénsense, por ejemplo, en un individuo al que hemos situado en un grupo de posibles delincuentes, a un recluta al que se lo 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.

6. RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, ob. cit, p. 598.

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

8. STC 25/1981, fundamento jurídico 5º.

9. *Ibidem*.

10. 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.

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”¹¹, 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”¹².

Constatados los peligros, se ha ido poniendo de manifiesto la necesidad de establecer los mecanismos de protección de la persona adecuados a la nueva agresión a su dignidad y derechos que la informática puede suponer. 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.

El Tribunal configura a partir del derecho general de la personalidad garantizado en la Ley fundamental de Bonn¹³, “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”¹⁴. 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”¹⁵. Es decir, el

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.

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

12. FROSINI, V., *Informática y Derecho*, trad. Jorge Guerrero y Marino Ayerra Redín, Temis, Bogotá, 1988, p. 34.

13. 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.

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

15. 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.

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”¹⁶. Por tanto, la necesidad de proteger mediante los adecuados instrumentos jurídicos los datos relativos a las personas, no depende tanto de si pertenecen o no a su ámbito íntimo, “cuanto a las posibilidades de elaboración e interrelación propias de la tecnología informática”¹⁷. 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.¹⁸

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”¹⁹. Lo importante es “la finalidad con la cual se reclaman los datos y que posibilidades de interconexión y de utilización existen”²⁰; y, sólo cuando estén claros estos puntos “se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa”²¹.

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.”²². 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”²³.

El derecho a la autodeterminación informativa pone el acento en el uso que se haga de las informaciones resultantes de interrelacionar determinados datos personales y del perfil que se obtenga. Por eso, lo que está en juego no es propiamente la intimidad de las personas, es su propia identidad. En este sentido apunta Vittorio Frosini: “la libertad informativa representa una nueva forma de desarrollo de la

16. *Ibidem*.

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

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

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

20. *Ibidem*.

21. *Ibidem*.

22. 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.

23. *Ibidem*.

libertad personal; no consiste únicamente en la libertad negativa del right 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’²⁴.

II. CONCEPTO Y CONTENIDO DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA. EL CASO “RENFE”

Al disponer el artículo 18.4 de la Constitución que “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”, ha incorporado una nueva garantía constitucional, en respuesta a las nuevas amenazas que las modernas tecnologías de la información suponen para la dignidad y los derechos de la persona. Esta garantía, que tradicionalmente se ha venido denominando derecho a la autodeterminación informativa²⁵, se caracteriza por constituir según el Tribunal Constitucional, por una parte un derecho instrumental de protección de otros derechos y, por otra, el derecho fundamental autónomo a controlar las informaciones que nos conciernen.²⁶

En mi opinión, más que hallarnos ante un derecho instrumental, nos encontramos ante un verdadero derecho fundamental autónomo íntimamente ligado al derecho a la intimidad —como también dice el Tribunal Constitucional—, pero que cumple, al igual que otros derechos fundamentales, en ocasiones, una función instrumental en cuanto que sirve para garantizar otras libertades.²⁷ No obstante y a fin de seguir más sencillamente su argumentación, respetaré la terminología y caracterización que de la libertad informática hace este Tribunal.

El derecho a la autodeterminación informativa, en cuanto derecho que realiza una función instrumental para la garantía de otros derechos fundamentales, arranca directamente del enunciado literal del artículo 18.4 de la Constitución. En dicho precepto se establecen limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos. El texto constitucional menciona expresamente dos de los derechos que podrían verse amenazados por un uso abusivo e ilegítimo de las nuevas tecnologías de la información, que nuestra Constitución llama “informáti-

24. FROSINI, V., *Informática y Derecho*, ob. cit., p. 23.

25. Aunque nuestro Tribunal Constitucional prefiera el de “libertad informática”. Así desde la STC 254/1993, de 20 de julio.

26. Reiteradamente, la Jurisprudencia del Tribunal Constitucional ha caracterizado el derecho a la autodeterminación informativa como un derecho instrumental ordenado a la garantía de otros derechos y un derecho fundamental autónomo con un contenido específico (SSTC 254/1993, de 20 de julio; 60/1998, de 16 de marzo y 105/1998, de 19 de junio, entre otras).

27. Piénsese, por ejemplo, en el derecho al secreto de las comunicaciones que puede cumplir la función de garantía del derecho a la intimidad cuando su contenido se refiera a aspectos de la vida privada de una persona.

ca”, los derechos al honor y a la intimidad personal y familiar. Otros como la libertad ideológica o religiosa, la libertad sindical, 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.

Por otra parte, en cuanto derecho fundamental autónomo, el derecho a la autodeterminación informativa es “el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes”²⁸ del uso torticero del tratamiento automatizado de datos personales.

Analizaré ahora ambos aspectos en relación con el supuesto que resolvió la sentencia del Tribunal Constitucional 11/1998, de 13 de enero.

El Tribunal Constitucional estimó el amparo interpuesto por un trabajador de RENFE contra la sentencia de la sala de lo 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.

1. Derecho de carácter instrumental (la función instrumental del derecho a la autodeterminación informativa)

Por cuanto el derecho a la autodeterminación informativa es un derecho que realiza una función instrumental, el análisis de la vulneración de los arts. 28.1 y 18.4 de la Constitución debe hacerse de forma conjunta.

El demandante de amparo pretendió que había sido conculcado su derecho a la libertad sindical y así lo confirmó el Tribunal Constitucional. El trabajador proporcionó a la empresa la información sobre su afiliación a un sindicato concreto 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, la empresa 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 es el único derecho afectado por la decisión empresarial. El propio derecho a la autodeterminación informativa resulta directamente afectado. Sin embargo y esto se pone claramente de manifiesto en este caso,

28. STC 254/1993, de 20 de julio.

a través de la protección de la persona frente al tratamiento automatizado de sus datos se están garantizando otros derechos, como por ejemplo la libertad sindical. Pero, es importante insistir en que la decisión empresarial como veremos en el apartado siguiente, vulnera directamente la garantía fundamental del artículo 18.4 de la Constitución.

Por tanto, a través de la protección constitucional a los datos personales automatizados, íntimos o no, se garantizan otras libertades que pueden resultar afectadas por el uso ilegítimo de esas informaciones. Por tanto, en este caso concreto, a través de la protección al dato de afiliación sindical que proporciona el derecho a la autodeterminación informativa se garantiza el contenido esencial de la libertad sindical.

Pero, ¿en qué consiste esa protección?

2. El derecho fundamental autónomo. Contenido del derecho a la autodeterminación informativa

En cuanto derecho fundamental autónomo, podemos distinguir dos elementos en el contenido mínimo del derecho a la autodeterminación informativa. 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 datos²⁹. El contenido propio del elemento negativo estaría formado por lo que se conocen como principios de calidad de los datos³⁰ mientras que el positivo lo formarían los derechos del titular de los datos.

2.1. Elemento negativo

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.³¹ 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

29. STC 254/1993, de 20 de julio.

30. 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.

31. No debe olvidarse que la informática ha supuesto grandes beneficios para el desarrollo de la humanidad. Piénsese en los avances conseguidos en todas las ciencias empíricas y de cálculo, en la medicina o en el avance que ha supuesto, en rapidez y facilidad de localización de documentación o jurisprudencia, en las autopistas de la información, etc.

origine y evitar que se vuelvan a producir.”³² Se trata de intentar “conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información”³³.

Los límites necesarios para garantizar ambos bienes, los que responden a la necesidad del tratamiento de informaciones personales³⁴ 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. A estos límites se les ha denominado tradicionalmente *principios de calidad de los datos*. Son los siguientes:

1.—*Principio de pertinencia*. 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, así, una “clara conexión entre la información que se recaba (...) y el objetivo para el que se solicitó”³⁵. 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 que aquellos que sean estrictamente necesarios en ese momento, aunque fuesen susceptibles de serlo para cumplir los objetivos futuros.

2.—*Principio de finalidad*.³⁶ Está 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 distintas de 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”³⁷.

Este principio significa, además, que una vez utilizados para la finalidad legal para la que hubiesen sido recabados no podrán ser reutilizados para el cumplimen-

32. MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, *Cuadernos y Debates* n° 43, Tecnos, Madrid, 1993, p. 39.

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

34. 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.

35. MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, op. cit., p. 65.

36. 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.

37. PÉREZ LUÑO, A. E., “Los derechos humanos en la sociedad tecnológica”, ob. cit., p. 168.

to 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.

3.—*Principio de veracidad y de exactitud.* 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 existir una perfecta correspondencia “entre el discurso que marcan los hechos y el que se trasmite al receptor de la información”³⁸.

4.—*Principio de lealtad.* Los datos personales deberán recogerse sin engaños o falsedades por parte de quien los solicita.

5.—*Principio de seguridad de los datos.* Deberán adoptarse las medidas necesarias para garantizar la seguridad de los datos personales evitando su alteración, pérdida, tratamiento o acceso no autorizados. La importancia de este principio, en orden a garantizar los derechos de los afectados, ha crecido en los últimos años. 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”³⁹, 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.

2.2. El elemento positivo

Como se ha enunciado es el derecho a controlar los propios datos. Este control se lleva a cabo a través de las siguientes facultades⁴⁰ que formarían el contenido del llamado *habeas data* o *habeas scriptum*.⁴¹

38. 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.

39. 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.

40. 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”.

41. 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”.

1.—*El derecho del titular de los datos a que se le informe* de los bancos de datos existentes, de su titularidad y finalidad. El derecho a la información 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 acerca de las cuestiones anteriores.

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”⁴². 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”⁴³.

3.—*El derecho de acceso* de los afectados a las informaciones que les conciernen, así como a “*la facultad de corrección y cancelación de los datos inexactos*”⁴⁴. Junto con los derechos de *rectificación y cancelación* de datos erróneos, el derecho de acceso 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 los instrumentos *a priori* de control sobre los datos personales, anteriores al momento en que éstos 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.

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.

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”, frente a los nuevos fenómenos abusivos que limitan la esfera informática de la libertad de la persona.

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

42. MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, ob. cit., p. 56.

43. 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.

44. PÉREZ LUÑO, A. E., *Derechos humanos, Estado de Derecho y Constitución*, ob. cit., p. 370.

Estamos ante tres derechos 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”⁴⁵.

4.—*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.

El derecho al olvido tiene por objeto contrarrestar uno de los riesgos más característicos del procesamiento informático de la información relativa a una persona; ya que supone la posibilidad de recuperar en un instante cualquier dato por insignificante que éste parezca, aún habiendo transcurrido decenas de años, lo que significa la desaparición de la garantía que suponía para la intimidad de las personas la fragilidad de la memoria humana.

En el caso que estamos analizando, RENFE descontó las retribuciones correspondientes a las jornadas de huelga al trabajador, basándose exclusivamente en el dato de afiliación sindical a uno de los sindicatos convocantes de la huelga. No se hizo ninguna otra averiguación, sino que aquellos trabajadores cuyos nombres estaban asociados a las claves informáticas de afiliación a dichos sindicatos, se les descontaron automáticamente los salarios correspondientes. La empresa presumió que el demandante había participado en la huelga por el simple hecho de pertenecer a uno de los sindicatos convocantes. Se produjo, por tanto, uno de los riesgos que el derecho a la autodeterminación informativa trata de evitar: “que la informatización de los datos personales propicie tratamientos discriminatorios”⁴⁶.

Asimismo, al utilizar el dato de afiliación sindical para descontar las retribuciones al trabajador se vulneró el principio de finalidad, que como se ha dicho forma parte del contenido del elemento negativo del derecho a la autodeterminación informativa. Recuérdese que el trabajador proporcionó dicho dato con la única finalidad de que se le descontase la cuota de afiliación sindical a favor de la organización sindical de su elección. Sin embargo, dicho dato sirvió para una finalidad “radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical”⁴⁷.

45. MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, ob. cit., p. 79.

46. STC 11/1998, de 13 de enero, fundamento jurídico quinto.

47. *Ibidem*.

Por otro lado, es completamente indiferente por lo que a la vulneración de los derechos mencionados se refiere, la concurrencia de dolo o culpa en la conducta empresarial. El elemento intencional es irrelevante y tampoco sería causa de justificación para ese comportamiento la gran dificultad alegada por la empresa para comprobar de forma efectiva quién participó y quién no en la huelga. Es indiferente al derecho a la autodeterminación informativa que la forma más sencilla de comprobación fuese la de acudir al fichero informático en el que figuraba la información relativa a la afiliación sindical de los trabajadores (lo que, además resultó errado, ya que el demandante no había participado en la huelga), ya que el contenido de este derecho prohíbe la utilización para finalidades diferentes o incompatibles con aquellas para las que se proporcionaron, los datos personales.

Además, en el presente caso⁴⁸ el uso desviado de esa información resulta especialmente grave, al enmarcarse el dato de la afiliación sindical dentro de aquellos que hacen referencia a la ideología de un individuo y que por tanto pertenecen a la categoría de los que se conocen como "datos sensibles". La consecuencia más importante que se deriva de tal calificación es que los principios que garantizan una determinada calidad de los datos, así como los derechos de los afectados, que configuran el elemento negativo y positivo del derecho a la autodeterminación informativa, deben exigirse, si cabe, con más rigor.

III. LA LEY 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES. LOS DERECHOS DEL INTERESADO

Frente a la regulación anterior, que siguiendo la dicción literal del art. 18.4 de la Constitución establecía como objeto de la Ley la limitación del uso de la informática para garantizar los derechos de los ciudadanos, la Ley 15/1999, influida por la Directiva 95/46/CE, establece como objetivo directo la garantía y protección, en lo referente al tratamiento de los datos personales, de las libertades públicas y los derechos fundamentales de las personas. ¿Supone este cambio de redacción el desplazamiento del centro de gravedad de la regulación de datos personales desde la informática a la persona?

De la lectura del artículo 1 de la Ley puede deducirse que lo importante ahora, más que limitar la informática, es garantizar de forma efectiva los derechos fundamentales de las personas. No obstante, conviene no olvidar que el objeto de limitar la informática en la ley anterior era precisamente garantizar esos mismos derechos, lo que por cierto es distinto del hecho de que esos derechos hubiesen quedado efectivamente garantizados.

48. El Tribunal Constitucional resolvió casos sustancialmente iguales, en base a argumentos semejantes, en las SSTC 60/1998, de 16 de marzo; 77/1998, de 31 de marzo o 105/1998, de 19 de junio, entre otras.

Por ello y pese a reconocer que la nueva redacción mejora la anterior por cuanto parece que, ahora sí, lo importante es la libertad y dignidad de la persona, en nada se habrá avanzado si los derechos de los afectados no gozan de plena eficacia frente a la anterior regulación caracterizada por las excepciones a aquéllos.⁴⁹ Por eso debe procederse al análisis de algunos aspectos principales de la Ley 15/1999, a fin de comprobar si puede mantenerse nuestra primera impresión, tan optimista.

1. Calidad de los datos

Por lo que se refiere a los principios de calidad de los datos, únicamente me referiré a la nueva redacción del principio de finalidad que 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 aquellas 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 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 utilizarán de forma incompatible con dichas finalidades”⁵⁰. 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 cientí-

49. Son de sobra conocidas las numerosas críticas doctrinales a la LORTAD. Así, por ejemplo, vid. PÉREZ LUÑO, A. E., *Manual de informática y Derecho*, Ariel, Madrid, 1996; MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, ob. cit.; DEL PESO NAVARRO, M. y RAMOS GONZÁLEZ, *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*, ob. cit., entre otros muchos.

50. Vid. HEREDERO HIGUERAS, M., *La Directiva comunitaria de protección de datos de carácter personal*, Aranzadi, Pamplona, 1997, en especial, pp. 103 a 105.

ficos al igual que hace la Directiva. 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.

2. Derechos de los afectados

1.—La primera novedad destacable en este apartado es la nueva regulación del derecho de información en la recogida de datos. Siguiendo la pauta marcada por la Directiva se establece la obligatoriedad de informar a los interesados cuando los datos no hayan sido recabados directamente de ellos. Se establecen sin embargo varias excepciones a esta obligación: cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o, finalmente, cuando los datos procedan de fuentes accesibles al público y se destinen a las actividades de publicidad o prospección comercial. Me centraré en las dos últimas.

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 cuándo nos encontramos ante uno u otro caso. Corresponderá así a la Agencia de Protección de Datos 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 público⁵¹ habían sido recogidos e iban a ser elaborados automatizadamente con una concreta finalidad. Expresamente se excluía la necesidad de solicitar el consentimiento del afectado cuando los datos tuvieran esta procedencia en cualquier caso. En la práctica esto suponía que estos datos se iban a utilizar, no sólo sin el consentimiento del afectado, sino también sin su conocimiento.

Ahora, aun cuando entre las excepciones al consentimiento del afectado siga figurando la de que los datos se recojan de fuentes accesibles al público, en los

51. Además, ahora se establecen cuáles son estas fuentes accesibles al público en el artículo 3.j) y se regulan específicamente en el artículo 28.

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”⁵², incluso en el supuesto en que no sea obligatorio el consentimiento del afectado. La más importante consecuencia de todo ello es, a mi juicio, 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, puesto 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, 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.—Las dudas que suscitaba la anterior regulación del consentimiento del afectado, acerca de la posibilidad de admisión del consentimiento implícito o tácito, parecen quedar desde ahora resultas. La adaptación a la directiva ha supuesto también en este aspecto una mejoría notable. No es que la anterior regulación admitiese cualquier consentimiento. No, el consentimiento debía 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

52. 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.

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

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 otra ocasión⁵⁵.

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 acuerdo con el artículo 6.2 en relación con el 7.6, ambos de la Ley Orgánica 15/1999.

Finalmente se exceptúa también el consentimiento del 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 legíti-

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. GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el Derecho español*, Universidad Carlos III de Madrid – Dykinson, Madrid, 1999, pp. 206 y ss.

mas. Así pues, 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 del “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 las 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 cuál debe ser el interés prevalente podría llegarse a la conclusión de que los intereses del mercado priman sobre los del interesado⁵⁷. Así por ejemplo prevalecería el interés legítimo, sin duda, del control de la morosidad o de evaluación de solvencia patrimonial⁵⁸ 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 límite se podría concretar de la forma que sigue: no podrá prescindirse del consentimiento del afectado, aun 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.

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, pp. 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.

58. Interpretación que corrobora el artículo 29 de la Ley que establece que “quienes se dedican 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...”.

3. El derecho de oposición es otra de las novedades de la Ley⁵⁹

Su importancia reside en que “se configura como un instrumento garante de carácter netamente preventivo o cautelar”⁶⁰ 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”⁶¹.

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”⁶² reconocidos en la Constitución.

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*.

4. Los datos sensibles

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 de la necesidad del consentimiento expreso y por escrito del interesado para tratar este tipo de datos. Lo positivo es que los ficheros mante-

59. 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.

60. 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.

61. *Ibidem*, p. 293.

62. 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.

nidos 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 Ley 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, o la libertad religiosa alcanzarán unas mayores cuotas de desarrollo, garantizando la mayor autodeterminación y libertad para las personas que integran estas instituciones.

5. Impugnación de valoraciones

Es novedosa también 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, barrio, etc. 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 éstos sean utilizados, por ejemplo, con fines comerciales o de *marketing* directo⁶³.

Ahora bien, y ésta 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.

No obstante 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 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, supongo, para que 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 lo 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”⁶⁴.

IV. CONCLUSIONES FINALES

Soy consciente de que son muchos los temas que no recojo y de que tienen, sin duda, gran interés. Sin embargo, no he pretendido en ningún momento abordarlos

63. 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.

64. MURILLO DE LA CUEVA, P. L., “Informática y protección de datos personales”, ob. cit., p. 83.

todos ya que no era el objetivo de este trabajo un análisis exhaustivo de la nueva Ley de Protección de Datos Personales. No obstante y puesto que aún no he respondido a la cuestión que se plantea en el título de este trabajo abordaré ahora, de forma muy breve y para concluir dos aspectos más de la Ley 15/1999, de 13 de diciembre.

Entre las “sombras” de la LORTAD⁶⁵ 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. Por lo que se refiere a la primera cuestión, las exclusiones del ámbito de aplicación de la nueva Ley son menos numerosas y más razonables, por lo que la valoración ha de ser 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 interesados⁶⁶. Se reproducen de forma prácticamente idéntica, 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 doctrina⁶⁷, que en algunos casos 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 afectados.

Por ello, aunque es razonable reconocer que ha habido avances importantes en aspectos determinados, especialmente por lo que se refiere al derecho de información, 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, no podemos concluir de

65. Vid. PÉREZ LUÑO, A. E., *Manual de Informática y Derecho*, ob. cit., pp. 61 y ss.

66. 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 por vía de 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.

67. 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 ha 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).

forma tan optimista como hemos empezado la última parte de este trabajo. Siguen existiendo demasiadas “y significativas excepciones”⁶⁸ que pueden afectar al contenido esencial del derecho a la autodeterminación informativa, que impiden que efectivamente éste pueda cumplir su 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.

Por lo tanto, de nada sirve enunciar en el artículo primero como objeto de la Ley *garantizar y proteger* los derechos fundamentales de las personas, si después los instrumentos que se ponen a disposición de los ciudadanos están tan limitados, que ni garantizan ni protegen. Nuevamente, el legislador se olvida, tal y como se dijo en la introducción, de que para garantizar y proteger efectivamente la dignidad, la libertad y la igualdad que nuestra Constitución consagra, han de establecerse mecanismos adecuados para que se equilibre la relación entre aquellos que controlan los grandes bancos de información personal y los demás, objeto de vigilancia y control.

68. *Ibidem*, p. 62.