

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL DERECHO COMUNITARIO*

Domingo Bello Janeiro

Sumario: I. Introducción: El derecho a la intimidad. II. Análisis de la Directiva 95/46/CE. II.1. Antecedentes. II.2. Aproximación a la Directiva. II.3. Contenido de la Directiva. II.4. Anexo. II.4.1. La Directiva 97/66/CE. II.4.2. Otra normativa comunitaria. III. Referencia al Derecho español. III.1. El artículo 18 de la Constitución. III.2. Breve análisis de la legislación española. IV. Conclusiones

I. INTRODUCCIÓN: EL DERECHO A LA INTIMIDAD

La información, entendida en sentido general, incluso la que revela aspectos íntimos de la personalidad, se ha convertido en los últimos tiempos en un auténtico bien de consumo. En la actualidad, y en todos los ámbitos de la vida, existe una verdadera demanda social de información; el político, el empresario, el comerciante, el profesional, necesitan cada día más una mayor y mejor información para el correcto desarrollo de su trabajo; incluso el propio ciudadano, en su dimensión más anónima, invierte gran parte de su tiempo en consumir información.

Se comprende, pues, que cualquier sociedad democrática que se precie, en la que el Estado Social y de Derecho debe asumir una posición ciertamente beligerante en la defensa y protección de los derechos de la persona, no pueda permanecer ajena, en palabras de J. M^a. ÁLVAREZ-CIENFUEGOS SUÁREZ¹, “a esta tensión dialéctica entre consumo de información y defensa de la personalidad”.

Ante la libertad de información, componente necesario de una sociedad libre, pluralista e igualitaria, la defensa del ciudadano y la protección de su esfera de intimidad personal y familiar constituye un criterio de legitimación política para toda sociedad democrática.

El origen histórico de la idea de intimidad, así entendida, surge, en opinión de la doctrina mayoritaria española, en el mismo momento en que se construye el Estado

* El texto original, que, con las debidas adaptaciones, constituye el presente trabajo, fue la conferencia pronunciada en el *Instituto Jurídico da Comunicação* de la Universidad de Coimbra el día 30 de junio de 2000, con ocasión de la entrega de Diplomas del 8º Curso de posgrado en Derecho de la Comunicación.

¹ ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M^a., “El Derecho a la intimidad y los registros informáticos de las Administraciones Públicas: problemas y garantías de su cesión”, ponencia presentada a las *Xornadas sobre o acceso dos cidadáns ós arquivos e rexistros públicos*, organizadas por la Escola Galega de Administración Pública, A Coruña, 22 y 23 de febrero de 2000.

liberal y aparece la burguesía y el individualismo², aunque su máximo esplendor y desarrollo tiene lugar a lo largo del siglo pasado³.

El derecho a la intimidad, para esta misma doctrina, se halla profundamente vinculado a la construcción y a la evolución de los derechos de la persona. Por intimidad entendemos aquel derecho del individuo a decidir por sí mismo, en qué medida o en qué circunstancias desea compartir con terceras personas sus pensamientos, sentimientos o impresiones y expresiones personales.

Por una parte, la intimidad facultaría al individuo para controlar eficazmente sus propias experiencias y vivencias, y, por contra, la confidencialidad sería el medio con el que proteger su propia intimidad.

La intimidad se refiere a la esfera más propia e interna del individuo, a diferencia de la vida privada, que hace referencia a una esfera de retiro y aislamiento, en la que los demás no tienen derecho a inmiscuirse⁴. Para la correcta delimitación de ambos derechos debe aceptarse la consideración del derecho a la vida privada como garantía de desarrollo de determinados aspectos de la existencia individual, alejada de la observación indiscreta de terceros y vedada al acceso de los mismos.

De acuerdo con E. VILARIÑO PINTOS⁵, por intimidad habrá de considerarse, simplemente, “el entorno inmediato y los aspectos más reservados de la propia persona y de su vida privada, en cuyo ámbito no puede legitimarse ningún tipo de intromisión y, por tanto, tampoco la obtención de datos relativos al mismo. Respecto a ellos la persona tiene derecho a la más absoluta protección, salvo, es obvio, que ella misma los haga públicos”.

En la actualidad, la lucha por la defensa de la vida privada se convirtió en una lucha por la defensa y el control de la información personal que le concierne a cada uno y que viene a revelar hasta los más íntimos comportamientos o hábitos de cada persona.

Se pueden distinguir con O'CALLAGHAN⁶ dos aspectos en el derecho a la intimidad:

a) Uno negativo, “como un modo de ser negativo de la persona respecto de los demás, que sería la exclusión del conocimiento ajeno de cuanto hace referencia a la propia persona”.

2 Así, entre otros, PÉREZ LUÑO, A. E., *Derechos humanos, Estado de Derecho y Constitución*, editorial Tecnos, Madrid, 1990, páginas 321 y siguientes; MARTÍNEZ DE PISÓN CAVERO, J., *El derecho a la intimidad en la jurisprudencia constitucional*, editorial Civitas, Madrid, 1993, páginas 40 y siguientes; MURILLO DE LA CUEVA, P. L., *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, páginas 49 y siguientes; BEJAR, H., *El ámbito íntimo*, Alianza Editorial, Madrid, 1990, páginas 58 y siguientes; GÓMEZ PAVÓN, P., *La intimidad como objeto de protección penal*, ediciones Akal, Madrid, 1989, páginas 12 y siguientes.

3 GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el Derecho español*, editorial Dykinson, Madrid, 1999, página 27.

4 En su evolución histórica, lo íntimo y lo privado se han ido desarrollando a costa de lo público. En palabras de BEJAR, H. (*El ámbito íntimo*, Alianza Editorial, Madrid, 1990, página 34), “lo privado es una categoría de un espacio abstraído de lo público (...) es el área que cae fuera de los márgenes de lo público, en la penumbra tejida por el silencio de la ley”.

5 VILARIÑO PINTOS, E., “Los derechos de la persona en el ámbito de las tecnologías de la información” en *El derecho a la intimidad y a la privacidad y las administraciones públicas*, varios autores dirigidos por BELLO JANEIRO, D. y coordinados por HEREDERO HIGUERAS, M., Escola Galega de Administración Pública, colección xornadas e seminarios núm. 24, Santiago de Compostela, 1999, página 20.

6 O'CALLAGHAN MUÑOZ, X., *Libertad de expresión y sus límites: honor, intimidad e imagen*, EDESA, Madrid, 1991, página 87.

b) Y otro positivo, “de control por su titular de los datos e información relativos a la propia persona”.

Sea como fuere, lo que en definitiva el derecho a la intimidad pretende es proteger lo que el profesor ALBALADEJO llama “círculo íntimo personal y familiar”⁷ y que nuestro Tribunal Supremo denomina como “la zona reservada de la persona y de su espíritu (...) que constituye un acervo y patrimonio de la persona más arcano”⁸.

II. ANÁLISIS DE LA DIRECTIVA 95/46/CE⁹

II.1 Antecedentes

El desarrollo fiable y sostenido de la Sociedad Mundial de la Información, tiene como prerequisite la existencia de elementos de seguridad y medios de control que merezcan la confianza de los ciudadanos.

La seguridad de la Infraestructura Mundial de la Información no es posible sin un estrecha colaboración de los agentes públicos y privados, al mismo tiempo que se produce una adecuada cooperación y armonización a nivel internacional.

Solamente si se sigue esta senda se podrán lograr las economías de escala imprescindibles para generalizar el uso de las nuevas tecnologías con una adecuada protección de los derechos individuales y colectivos, en especial el derecho a la protección a la intimidad.

La idea de una Directiva de protección de datos aparece por primera vez en 1974, cuando sólo existían dos leyes sobre protección de datos, en el Land de Hesse (1970) y en Suecia (1972).

En 1974, habiendo mostrado ya la Comisión cierta preocupación por la incidencia de la informática en el ámbito de los derechos y libertades, el Parlamento elaboró un estudio bajo la dirección de lord Mansfield, presentado finalmente en febrero de 1975. Esta iniciativa inaugura lo que podríamos llamar “la larga marcha hacia la Directiva”¹⁰, cuyos hitos sucesivos serían:

- * Resolución de 1979 del Parlamento
- * Recomendación de la Comisión de 1981
- * Resolución del Parlamento de 1982
- * Propuestas de 1990/1992 de la Comisión.

Por otra parte la única norma internacional vinculante en materia de protección de datos personales era el Convenio 108 del Consejo de Europa, de 28 de enero de 1981,

7 ALBALADEJO, *Derecho civil*, tomo I, volumen segundo, editorial Bosch, Barcelona, 1991, página 66.

8 Sentencia del Tribunal Supremo de 13 de marzo de 1989, fundamento jurídico primero.

9 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas*, nº L 281 de 23 de noviembre de 1995, página 31-50.

10 HEREDERO HIGUERAS, M., “La protección de los datos de carácter personal en el Proyecto de Ley Orgánica de adaptación de la Ley Orgánica 5/1992, de 29 de octubre, a la Directiva 95/46/CE” en *El derecho a la intimidad y la privacidad y las Administraciones Públicas*, Escola Galega de Administración Pública, Colección Xornadas e Seminarios núm. 24, Santiago de Compostela, 1999, página 81.

para la protección de las personas con respecto al tratamiento de datos de carácter personal, hecho en Estrasburgo.

II.2 Aproximación a la directiva 95/46/CE

Son tantos y de tanta trascendencia los intereses que confluyen en el tema de la protección de datos personales en el Derecho Comunitario que se hace necesaria una regulación exhaustiva. Así, de forma simultánea nos encontramos con que debe lograrse un punto de equilibrio entre:

- * los intereses de las personas físicas como principales afectados, pues es la utilización de sus propios datos personales la que exige una regulación.
- * los intereses de los Estados miembros, siempre reacios a abdicar su soberanía.
- * el continuo desarrollo en las nuevas tecnologías con el gran valor añadido que supone para nuestra sociedad de la información y de las telecomunicaciones.

Los sistemas de tratamiento de datos deben fundamentarse en el servicio que prestan a las personas, por lo que deben, sin que importe la nacionalidad o la residencia, respetar las libertades y derechos fundamentales, en particular, la intimidad, además de contribuir al desarrollo económico y social, así como al bienestar de los individuos.

El continuo crecimiento en el tratamiento de datos personales en todos los sectores de actividad económica y social cuenta con una gran colaboración de las nuevas tecnologías de la información que facilitan considerablemente el tratamiento e intercambio de dichos datos¹¹.

A todo esto debemos añadir el notable aumento de los flujos transfronterizos de datos personales entre todos los agentes públicos y privados de la vida económica y social de los Estados miembros. En especial, las administraciones de los diferentes Estados miembros, en aplicación del Derecho comunitario, deben colaborar en el intercambio de los datos personales en el marco del espacio sin fronteras que constituye el mercado interior¹².

El nivel de protección de los derechos y libertades de las personas debe ser equivalente en todos los Estados miembros, por lo que la Directiva se justifica en la necesidad de aproximar las grandes diferencias entre las legislaciones nacionales aplicables.

Estas considerables diferencias legislativas podrían impedir la transmisión de datos personales entre los Estados miembros por lo que podrían falsear la competencia, e incluso, obstaculizar el ejercicio de actividades económicas¹³.

II.3 Contenido de la directiva 95/46/CE

El contenido de la Directiva se puede sistematizar a grandes trazos en los siguientes términos:

- * Objeto y fin de la Directiva
- * Ámbito de aplicación

¹¹ Directiva 95/46, Considerando 2.

¹² *Ibidem*, Considerando 5.

¹³ *Ibidem*, Considerando 7.

- * Derechos del interesado
- * Obligaciones del responsable
- * Excepciones y limitaciones
- * Órganos
- * Transferencia de datos a terceros países
- * Códigos de conducta

Desde el punto de vista formal, el texto se concibe como un conjunto de proposiciones normativas de aplicación general, sin perjuicio de que algunas de ellas contengan sus propias derogaciones o modulaciones¹⁴.

II.3.1 Objeto y fin de la Directiva

Dos son los objetivos de la Directiva:

1. El primero: que los Estados miembros garanticen la protección de las libertades y de los derechos fundamentales de las personas físicas, particularmente del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. En segundo lugar: impedir la restricción o prohibición de la libre circulación de datos personales entre los Estados miembros, basándose en la protección de los anteriores derechos y libertades.

Ambos objetivos son equiparados en cuanto a su importancia y, con carácter general, no debe prevalecer uno sobre otro¹⁵.

II.3.2 Ámbito de aplicación

- * Ámbito de aplicación *ratione materiae*

El artículo 2 a) entiende por datos personales “toda información sobre una persona física identificada o identificable (el interesado); considerándose identificable toda persona cuya intimidad pueda determinarse, directa o indirectamente...”

La inclusión del término “indirectamente” pretende que la protección se extienda a toda persona que, de una forma u otra, por asociación de conceptos o contenidos, aunque no se haga una directa referencia a ella, pueda ser identificada o identificable¹⁶.

También se inscriben en el ámbito de aplicación por razón de la materia los apartados b) y c) del mismo artículo, definiendo los conceptos de tratamiento de datos personales y fichero de datos personales.

- * Ámbito de aplicación *ratione personae*

Es descrito en los apartados d) a g) del artículo 2 de la Directiva.

- * Ámbito de aplicación *ratione loci*

Se recoge en los artículos 4, 25 y 26 de la Directiva.

14 HEREDERO HIGUERAS, M., *Op. cit.*, páginas 88 y 89.

15 GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el Derecho español*, Dykinson, Madrid, 1999, página 295.

16 DAVARA RODRÍGUEZ, M. A., *La protección de datos en Europa*, ICADE, Madrid, 1998, página 47.

El artículo 4 se refiere a la cuestión del Derecho nacional aplicable. En el marco de la Directiva los Estados miembros deberán aplicar las disposiciones nacionales no sólo a todo tratamiento de datos personales efectuado por responsables establecidos en el territorio del Estado miembro, sino también cuando los responsables del tratamiento recurran a medios situados en el territorio de dicho Estado miembro, especialmente para recoger datos personales¹⁷.

Los artículos 25 y 26 a los principios y excepciones relativas a la transferencia de datos personales a terceros países.

II.3.3 Derechos del interesado

En los artículos 10 y 11 se recoge el principio de **información** del interesado, refiriéndose el primero de ellos a la obtención en caso de que los datos hayan sido recabados por el propio interesado y el segundo al supuesto de que no hayan sido recabados por él. En ambos casos se persigue que el interesado esté informado sobre:

1. la identidad del responsable del tratamiento y, en su caso, de su representante.
2. los fines del tratamiento de que van a ser objeto los datos.
3. cualquier otra información, tal como:
 - a) los destinatarios de los datos
 - b) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para el interesado una negativa a responder
 - c) la existencia de derechos de acceso y rectificación de los datos que le conciernen

Todo ello enmarcado en un contexto de tratamiento de datos “leal” respecto al interesado.

No obstante, en el caso de que los datos no hayan sido recabados por el propio interesado establece el artículo 11 que no se aplicarán estas disposiciones cuando:

* el tratamiento se realice con fines estadísticos o de investigación histórica o científica.

* la información al interesado resulte imposible o exija esfuerzos desproporcionados, lo cual no está justificado ya que puede servir en cualquier caso de excusa para eludir la obligación de informar al interesado, dada la dificultad de demostrar lo contrario¹⁸.

* el registro o la comunicación a un tercero estén prescritos por ley.

Estableciéndose, naturalmente, en tales casos las garantías adecuadas por los Estados miembros, aunque éstas no se llegan a especificar.

El artículo 12 introduce en el derecho de **acceso** del interesado a los datos la particularidad de que sea “con una periodicidad razonable y sin retrasos ni gastos excesivos”, lo que merece un par de comentarios:

17 Grupo de Trabajo sobre protección de datos del artículo 29, Dictamen 4/2000, aprobado el 16 de mayo, sobre el nivel de protección que proporcionan los principios de “puerto seguro”, página 3.

18 PRIETO GUTIÉRREZ, J. M., “La Directiva 95/46/CEE como criterio unificador” en *Informática y Derecho. Revista iberoamericana de Derecho informático*, nº 23-26, UNED, Centro Regional de Extremadura, Mérida, 1998, página 1107.

* No se establecen limitaciones en cuanto al ejercicio de este derecho, aunque se haga referencia a una “periodicidad razonable”, pero sin que se concrete un período de tiempo determinado¹⁹.

* Se abre la posibilidad de que el titular del fichero pueda cobrar una cantidad no excesiva por el ejercicio del derecho de acceso del interesado. Incluso esa cantidad podría ser la resultante del cálculo del coste que ese derecho de acceso conlleve en su repercusión sobre el titular del fichero²⁰.

Asimismo, el mismo artículo regula también el derecho de **rectificación, supresión o bloqueo** de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, contemplando al mismo tiempo la obligación de notificar el hecho de haber practicado tales actividades conforme a lo solicitado por el interesado.

El artículo 14 recoge el derecho de **oposición** del interesado, una de las más valiosas aportaciones de la Directiva. Su importancia reside en que se configura como un instrumento garante de carácter netamente preventivo o cautelar frente a las soluciones típicas de remedio *a posteriori* propias de los sistemas judiciales²¹.

La Directiva reconoce al interesado el derecho a oponerse al menos en los siguientes casos:

1. cuando sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se le comuniquen los datos

2. cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se le comuniquen los datos, siempre que no prevalezca el interés o los derechos fundamentales del interesado

En ambos casos se establece la salvedad de que las legislaciones nacionales dispongan otra cosa, lo cual supone una traba para el margen de efectividad del derecho de oposición. Además, a continuación se recoge la imposibilidad de tratar los datos sobre los que se haya mantenido una oposición injustificada.

La regulación del derecho de oposición no está en absoluto exenta de críticas: este derecho sería realmente de gran importancia si se contemplara en el sentido lato de la palabra. En verdad se limita la efectividad de este derecho a unos cuantos supuestos muy concretos, tal vez con el ánimo de mitigar el amplio margen concedido al principio del consentimiento del artículo 7 donde se utilizan expresiones muy vagas de amplio contenido²².

3. El tercer supuesto en que el interesado puede oponerse se da cuando el responsable prevea un tratamiento destinado a la prospección, teniendo derecho a ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección y a que se le ofrezca expresamente el derecho a la oposición.

Cuando la Directiva habla de “prospección” está haciendo referencia a los ficheros mantenidos con fines de publicidad y de marketing directo.

19 *Ibidem*, página 1109.

20 DAVARA RODRÍGUEZ, M. A., *Op. cit.*, página 52.

21 CORRIPIO GIL-DELGADO, R., “Las nociones de interés público e interés legítimo en relación al derecho de oposición del interesado” en *Jornadas sobre el Derecho español de Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, página 287.

22 PRIETO GUTIÉRREZ, J. M., *Op. cit.*, páginas 1110 y 1111.

El artículo 15 de la Directiva indica que no podrán tomarse **decisiones individuales automatizadas** destinadas a “evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.”.

En este caso cabría preguntarse qué se entiende por “decisiones individuales automatizadas”, ya que el referido precepto dice “una decisión...que se base únicamente en un tratamiento automatizado de datos...”. Una interpretación muy cicatera de este artículo 15 llevaría incluso a presumir como no válidas múltiples operaciones electrónicas que se encuentran fuertemente arraigadas en las relaciones económicas²³.

II.3.4 Obligaciones del responsable del tratamiento

En primer lugar, para garantizar la **confidencialidad** del tratamiento el artículo 16 exige que las personas que actúen bajo la responsabilidad del encargado o responsable del tratamiento solamente podrán tratar datos personales a los que tengan acceso cuando se lo encargue el responsable del tratamiento o actúen en virtud de imperativo legal.

La segunda obligación expresamente impuesta al responsable del fichero es en materia de **seguridad**. En efecto, el artículo 17 dispone que es a él a quien corresponde establecer las medidas de seguridad adecuadas, técnicas y de organización, para proteger los datos de su destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados.

Asimismo, el responsable del tratamiento tiene la obligación de **notificación** a la Autoridad de control, de manera previa al tratamiento, la realización del mismo (artículo 18). La Directiva también especifica el contenido que ha de contener dicha notificación (artículo 19).

II.3.5 Excepciones y limitaciones

En el artículo 13 se relacionan las excepciones y limitaciones aplicables a los derechos y obligaciones que la Directiva establece.

Con tales medidas se trata de salvaguardar una serie de intereses, justificándose las relativas a la Seguridad del Estado, la Defensa y la Seguridad Pública, en cuanto son intereses que deben prevalecer por encima de los particulares en beneficio del conjunto de la Comunidad.

Sin embargo, no compartimos tal justificación al privar al interesado de unos derechos y garantías con relación al tratamiento de sus datos personales frente a unos intereses que afectan a infracciones penales o deontológicas, intereses económicos o financieros “importantes” o a funciones de control, inspecciones o reglamentarias relacionadas con las anteriores. Intereses que habría que examinar caso por caso, a fin de determinar si realmente han de prevalecer por encima del derecho del interesado o no²⁴.

II.3.6 Órganos

A) LA AUTORIDAD DE CONTROL

En el artículo 28 la Directiva prevé la creación de una Autoridad de Control independiente en cada uno de los Estados miembros con la fundamental función de vigilar y controlar, en sus respectivos territorios, la aplicación de las disposiciones en ella contenidas.

23 DAVARA RODRÍGUEZ, M. A., *Op. cit.*, páginas 52 y 53.

24 PRIETO GUTIÉRREZ, J. M., *Op. cit.*, página 1110.

El artículo 28 no regula la estructura orgánica de la Autoridad, aunque entiende que ésta constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales²⁵.

La Directiva no se inclina por un concreto modelo de órgano -colegiado o unipersonal-, ni establece mayores exigencias que la de que en el ejercicio de sus funciones actúe con total independencia. Por lo que se refiere a sus funciones y potestades, la Norma europea las enumera pormenorizadamente.

Cabe destacar que el reseñado artículo 28 intenta asegurar:

1. la independencia del Órgano de Control para que pueda realizar sus funciones sin ningún tipo de condicionantes y sin distinción entre ficheros de titularidad pública o privada.

2. la participación de la Autoridad de Control en la elaboración de reglamentos u otras medidas administrativas que se vayan a tomar cuando éstas se refieran al tratamiento de datos de carácter personal.

3. el otorgamiento de poderes de investigación, intervención y capacidad procesal que permita hacer efectiva la intervención y control que la Ley le asigne, concediendo al Órgano la necesaria personalidad jurídica para que pueda llevar a cabo sus funciones²⁶.

B) EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

La Directiva dedica dos artículos a la regulación del Grupo de Protección: el artículo 29, a fin de determinar la formación y funcionamiento de tal órgano; y el artículo 30, en el que se determinan sus funciones.

Se trata de un órgano destinado a ser el gran catalizador entre los Estados miembros de la UE, tal como se esboza en el Considerando 65 de la Directiva²⁷.

El Grupo se configura como un organismo de carácter consultivo e independiente cuyas funciones se resumen en asesorar a la Comisión Europea en materia de protección de datos y contribuir a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la Directiva.

El Grupo de Protección está compuesto por:

* un representante de la Autoridad o Autoridades de Control designadas por cada Estado miembro.

* un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios.

* un representante de la Comisión Europea.

II.3.7 Transferencia de datos a terceros países

Los artículos 25 y 26 se refieren a los principios y excepciones en relación a la transferencia de datos a países terceros.

Merece la pena destacar que se establece el principio general de la transferencia de datos a terceros países, según el cual los Estados miembros sólo podrán transmitir

25 Preámbulo de la Directiva 95/46, Considerando 62.

26 DAVARA RODRÍGUEZ, M. A., *Op. cit.*, páginas 57 y 58.

27 Preámbulo de la Directiva 95/46, Considerando 65.

datos personales a un país no comunitario cuando éste garantice un “nivel de protección adecuado”. Sin embargo, la transferencia de datos entre Estados miembros se adecuará a un criterio diferente: el de un “nivel equivalente de protección”.

No significa lo mismo “equivalente” que “adecuado”, ya que a los Estados miembros se les exige, para que los datos puedan circular libremente por sus territorios alcanzar un nivel equivalente al del Estado transmisor²⁸, cuando la transmisión de datos se produce hacia un país no comunitario sólo se exige que se satisfaga un estándar mínimo de protección²⁹.

II.3.8 Códigos de conducta

Tanto el artículo 27 como el Considerando 61 de la Directiva, vienen a definir lo que dan en llamar “Códigos de Conducta”, como acuerdos establecidos por las asociaciones profesionales y demás organizaciones representantes de responsables de tratamiento, para la correcta aplicación de las disposiciones nacionales adoptadas en los Estados miembros en aplicación de la Directiva.

II.4 Anexo

El rápido desarrollo de las infraestructuras de la información, tanto a nivel nacional como internacional hace necesaria la existencia de una red sin fisuras para las comunicaciones y el acceso a los datos de carácter personal en todos los países del mundo.

Ante los efectos, de tanto calado, que está teniendo esta red de información y comunicaciones sobre el desarrollo económico y el comercio mundial, sus usuarios deben tener total confianza en la seguridad de la información y las infraestructuras, redes y sistemas de comunicaciones; en la confidencialidad, integridad y disponibilidad de los datos sobre ellos; y en la capacidad de demostrar el origen y la recepción de los datos³⁰.

II.4.1 La Directiva 97/66/CE

De especial significación en el ámbito de la protección de datos en el sector de las telecomunicaciones es la Directiva 97/66/CE del Parlamento europeo y del Consejo de 15 de diciembre de 1997. Dicha Directiva regula el tratamiento de los datos personales y de la protección de la intimidad en el ámbito de las telecomunicaciones.

Responde esta Directiva a dos circunstancias:

* las nuevas redes digitales públicas avanzadas de telecomunicación están creando necesidades específicas en materias de protección de datos personales y de la intimidad de los usuarios.

* la sociedad de la información en continuo desarrollo implica la introducción de nuevos servicios de telecomunicación con un desarrollo transfronterizo.

Pues bien, el éxito de la utilización de estas nuevas formas de las telecomunicaciones depende en gran parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad.

²⁸ *Ibidem*, Considerando 8.

²⁹ ESTADELLA YUSTE, O., “La transmisión internacional de datos personales y su control” en *Jornadas sobre el Derecho español de Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, página 202.

³⁰ Recomendación del Consejo en relación con las Directrices para una política criptográfica, 27 de marzo de 1997.

Las disposiciones de la Directiva 97/66 están destinadas a proteger, como complemento de la Directiva 95/46, los derechos fundamentales de las personas físicas, especialmente su derecho a la intimidad, al tiempo que a los intereses legítimos de las personas jurídicas.

En cuanto a la aplicación de esta Directiva los Estados deberían poner en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma a más tardar, según su artículo 15.1, el 24 de octubre de 1998³¹. Si bien en el artículo 5.1 se establece una prórroga hasta el 24 de octubre de 2000³².

II.4.2 Otra normativa comunitaria

La Comisión presentó el 14 de julio de 1999 una **propuesta de Reglamento** del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos³³.

Asimismo, hay que destacar la **Directiva 1999/93/CE** del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica³⁴. Con esta Directiva se busca incrementar la confianza de los usuarios en la comunicación y el comercio electrónico.

Para esto se determina que los proveedores de servicios de certificación deben observar, obligatoriamente, la normativa sobre protección de datos y el respeto de la intimidad, por lo que sólo podrán recabar datos personales directamente del titular de los mismos o con previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y mantenimiento del certificado³⁵.

Por otra parte existe también la **Posición Común (CE) n° 22/2000**, de 28 de febrero, con vistas a la adopción de una Directiva sobre el comercio electrónico³⁶. La aplicación y ejecución de la futura Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios.

III. REFERENCIA AL DERECHO ESPAÑOL

III.1. El Artículo 18 de la Constitución Española

Con la aprobación de la Constitución española en 1978 se consagra el derecho a la intimidad como derecho de la persona, junto al honor y a la propia imagen. La vulneración de este derecho vendrá de la manipulación de la persona, de la investigación o de la utilización desviada de la información que le concierne.

31 *Diario Oficial de las Comunidades Europeas*, n° L 024 de 30/01/1998, página 0001-0008.

32 *Ibidem*, “Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al pública (...)”.

33 [COM (1999) 337 final].

34 *Diario oficial de las Comunidades Europeas*, n° L 013 de 19/01/2000, páginas 0012-0020.

35 *Ibidem*, artículo 8.3.

36 *Diario Oficial de las Comunidades Europeas*, n° C 128 de 08/05/2000, página 0032.

Entre los llamados “derechos fundamentales de tercera generación”³⁷ se halla el “derecho a la intimidad”, “derecho a la privacidad”, “derecho de privacidad”, “derecho a la vida privada”, etc.³⁸ El artículo 18 de la Constitución española reconoce una variedad de modalidades de este derecho que sólo tienen en común el marco genérico que, con carácter mediato o indirecto protegen: las circunstancias y antecedentes de la vida particular de las personas, el contenido de los mensajes objeto de comunicación y correspondencia, la información personal registrada en soporte informático, son otras tantas manifestaciones de un mismo bien jurídico protegido.

En todos estos supuestos, el interesado goza de un derecho de disposición, bien en cuanto a la difusión de los hechos de su vida personal por los medios de comunicación social, bien por lo que respecta a la captación y subsiguiente registro y tratamiento en soporte informático³⁹.

La incidencia de las nuevas tecnologías en los derechos de la persona formula el problema de si la construcción tradicional del derecho a la intimidad puede o no sustentar la protección jurídica de la persona y sus bienes más esenciales frente a las agresiones surgidas con la aparición de la sociedad informatizada.

Los ordenadores han hecho evolucionar a la sociedad, su utilización abusiva comenzó a invadir la intimidad y la vida privada de los individuos. Por lo que, si se quiere mantener una eficaz protección, el derecho a la intimidad necesita una reformulación jurídica y conceptual adaptada a las nuevas amenazas tecnológicas y científicas

37 La tercera generación de derechos está integrada por derechos tales como el derecho a la paz, al medio ambiente, los derechos de los consumidores, a la calidad de vida, a la autodeterminación informativa, etc. Surgen como respuesta al fenómeno de *liberties pollution* o de la contaminación de libertades, esto es, ante la situación de “erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías” (PÉREZ LUÑO, A. E., “Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data”, en GARCÍA SAN MIGUEL, L. (Ed.), *Estudios sobre el derecho a la intimidad*, editorial Tecnos, Madrid, 1992, página 37).

Su fundamentación la encontramos, de acuerdo con GARRIGA DOMÍNGUEZ, A. (*La protección de los datos...*, cit., página 25), en el valor jurídico solidaridad, frente a los valores libertad e igualdad que fundamentan los derechos de la primera y segunda generación, respectivamente.

38 En cuanto a los “derechos humanos de la tercera generación”, la sentencia del Tribunal Constitucional 214/1991, de 11 de noviembre, reconoce por vez primera la legitimación activa para interponer un recurso de amparo constitucional, no de manera exclusiva al ofendido o a sus herederos, sino que la extiende a toda persona natural o jurídica que invoque un interés legítimo y, en este supuesto concreto, a la persona perteneciente a un grupo étnico o social determinado. De esta forma el Tribunal Constitucional trata de asegurar la protección y la tutela judicial de los derechos de las minorías que de no ser así quedarían claramente desprotegidos. Esta sentencia refleja, y de ahí su relevancia y notoriedad, “hasta que punto la solidaridad que nace de la condición de pertenencia del recurrente al grupo étnico que ha padecido la ofensa es condición suficiente para reconocer su legitimación procesal en cuanto titular de un interés legítimo” (VIDAL GIL, E. J., “Sobre los derechos de solidaridad. Del Estado liberal al social y democrático de Derecho”, en *Anuario de Filosofía del Derecho*, Nueva Época, tomo X, Ministerio de Justicia, Madrid, 1993, páginas 107 y 108). Así la solidaridad termina convirtiéndose en “un instrumento clave para la comprensión de la aplicación y para la interpretación de los derechos” (PECES-BARBA MARTÍNEZ, G., *CURSO DE DERECHOS FUNDAMENTALES, (I) TEORÍA GENERAL*, Eudema Universidad, Madrid, 1991, página 240).

39 La jurisprudencia más reciente del Tribunal Constitucional, concretamente su sentencia 134/1999, de 15 de junio (Sala Primera) -BOE de 18 de agosto de 1999-, reconoce este derecho de disposición sobre los hechos y circunstancias de la vida privada, pero de tal manera que no es lícito interpretar un acto de disposición expresa o presunta de unos hechos concretos, haciéndolo extensivo a la totalidad de la vida particular de una persona, aun cuando, en principio, todos los hechos de la vida del interesado pudieran ser de interés público.

En el caso del uso de los datos informatizados, la doctrina y la jurisprudencia son unánimes en reconocer una variante de este derecho de disposición en el llamado de autodeterminación informática. La progresiva irrupción de las tecnologías de la información en las comunicaciones (telefonía digital, correo electrónico, redes interactivas) confiere cierto carácter difuso a las fronteras que separan, en su caso, el secreto de la correspondencia, el secreto de las comunicaciones y la disposición sobre la vida privada y la autodeterminación informática.

que se ciñen sobre la persona, para que avancen los instrumentos legales de tutela paralelamente a la evolución de la sociedad.

Una Constitución tan reciente como la española no podía desconocer la importancia que los avances técnicos y científicos representan para el hombre, y su incidencia en los derechos y libertades de la persona.

Así pues, dentro de los derechos fundamentales, el artículo 18.4 de la Constitución viene a dar protección a los datos automatizados, si bien desde una disposición de carácter general, al establecer 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”.

El principal aspecto de la tutela de los derechos de las personas frente al uso de la informática a la que se refiere en artículo 18.4 de la Constitución española es, sin duda, la protección de los datos personales; y constituye ciertamente una preocupación novedosa en nuestro ordenamiento jurídico.

La previsión constitucional de la tutela de los derechos frente al uso de la informática se proyecta especialmente sobre los datos personales e implica derechos y garantías para los titulares de estos datos de carácter personal; al tiempo que supone para quienes lo recogen, tratan, transmiten, ceden o conservan, una serie de obligaciones en lo que se refiere a la calidad y seguridad de la información así como a las condiciones en que pueden utilizarla, almacenarla o cederla⁴⁰.

El ámbito de defensa que esta norma hace de los derechos de los ciudadanos frente al uso de la informática alcanza, prácticamente, a todos y cada uno de los derechos tipificados como fundamentales por la Sección Primera del Capítulo Segundo del Título Primero de la Constitución; con lo que no sólo no se compromete de manera expresa a defender el honor y la intimidad personal y familiar de los ciudadanos, sino que invoca como “zona protegida” del abuso informático el pleno ejercicio de sus derechos⁴¹.

Estas posibilidades que nos ofrece nuestra Constitución no se encuentran, por lo general, en los textos constitucionales de otros Estados europeos que, paradójicamente y a pesar de esta carencia, hace ya tiempo que han aprobado leyes específicas de protección de datos personales⁴², contando por tanto con una larga experiencia en las técnicas de control de ficheros informáticos sobre tales datos⁴³.

40 MURILLO DE LA CUEVA, P. L. *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

41 Ya el Tribunal Constitucional español, en su sentencia 254/1993, de 20 de julio, al comentar la incidencia del Convenio del Consejo de Europa de 1981 en la interpretación del artículo 18.4 de nuestra Constitución, recuerda que este precepto tiene como finalidad garantizar a toda persona física el respeto de sus derechos y libertades fundamentales, y en especial de su derecho a la vida privada respecto del tratamiento automatizado de sus datos personales, por esta razón, la cuestión referida en el recurso relativa a la negativa de un Gobernador Civil a proporcionar información a un ciudadano de los datos personales existentes sobre su persona en los ficheros informatizados de la policía, viene a constituir una vulneración del derecho fundamental a la intimidad personal y familiar.

La conclusión a que llega el Alto Tribunal, en aplicación del precitado Convenio, consiste en reconocer que las facultades de información constituyen parte del contenido del derecho a la intimidad, el cual vincula directamente a todos los poderes públicos.

En otra sentencia más reciente de 13 de enero de 1998, el Tribunal Constitucional señala la vulneración del artículo 18.4 de la Constitución cuando los datos facilitados por un trabajador a la empresa, con objeto de conocer su afiliación sindical, se utilizan por la empresa para otros fines distintos, sin obtener previamente el consentimiento del afectado.

42 Sobre las normas internacionales en esta materia, se pueden citar: la Ley de Privacidad de Estados Unidos de 1974; la Ley francesa de 1978, relativa a la informática, los ficheros y las libertades; la Ley de Registros Privados de Dinamarca de 1978; la Ley de datos sueca de 1982; la Ley de Protección de Datos del

III.2. Breve análisis de la Legislación Española

Además del referido artículo 18.2 de la Constitución, que contiene una referencia expresa a la protección de la intimidad personal y familiar, el ordenamiento jurídico español ofrece un bloque de normas, cada día más extenso, dirigido a proteger la esfera íntima de las personas frente a la utilización de sistemas informáticos para el almacenamiento y tratamiento de datos de carácter personal.

La Constitución española de 1978, es junto con la portuguesa de 1976, es una de las primeras en recoger como derecho fundamental la protección de los datos personales frente al uso de la informática; pese a esto, la adopción de normas concretas sobre la materia se retrasó hasta 1992.

Así, junto al Convenio 108 del Consejo de Europa⁴⁴, para la protección de las personas respecto al tratamiento de datos de carácter personal, cuyo valor normativo deriva del artículo 10 de la Constitución⁴⁵, debe citarse, en primer término, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD)⁴⁶, que ha derogado la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD)⁴⁷.

Reino Unido de 1984, que define la intimidad como el derecho a estar sólo, derecho a no ser molestado, a guardar reserva sobre la propia vida privada; la Ley de Protección de Datos de Hesse de 1986; la Ley de Registros de Personas de Noruega de 1987; la Ley austriaca de protección de datos personales de 1978, reformada en el año 1986.

En todas ellas se aprecia una doctrina común dirigida principalmente a garantizar la legitimidad de la elaboración y almacenamiento de datos nominativos, el derecho de los ciudadanos al acceso, rectificación y, en su caso, destrucción de datos nominativos o sensibles.

A modo de ejemplo, la Ley austriaca proclama el derecho fundamental a la protección de datos personales y el Tribunal Constitucional de este mismo país señalaría en 1988 que "la libertad de información no es absoluta y puede ser limitada en interés de la vida privada o de cualquier otro derecho fundamental".

43 Los instrumentos internacionales sobre derechos humanos son claros al establecer la necesidad de proteger a la persona respecto a esos datos:

a) La Declaración Universal de Derechos Humanos: el artículo 12 prohíbe la injerencia arbitraria en la vida privada de las personas, su familia, su domicilio o su correspondencia y los ataques a su honra o a su reputación y establece el derecho de la persona a la protección de la ley contra tales injerencias y ataques.

b) El Pacto Internacional de Derechos Civiles y Políticos: el artículo 17 se manifiesta en los mismos términos que el artículo 12 de la Declaración Universal, añadiendo la prohibición de las injerencias ilegales.

c) El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales: el artículo 8 establece el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Prohíbe, igualmente, la injerencia de la autoridad pública en el ejercicio de este derecho, cuando no esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y de las libertades de los demás.

d) La Declaración Americana de los Derechos del Hombre: el artículo 5 establece el derecho de toda persona a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

44 De 28 de enero de 1981, ratificado por España el 27 de enero de 1984 y publicado en el *BOE* de 15 de noviembre de 1985.

45 A tenor del artículo 10.2 de la Constitución Española "las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y Acuerdos internacionales sobre las mismas materias ratificados por España".

46 Publicada en el *BOE* de 14 de diciembre de 1999.

47 Publicada en el *BOE* de 31 de octubre de 1992. Para un estudio pormenorizado de esta Ley, *vid. HEREDERO IGLESIAS, M., La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de carácter personal. Comentarios y Textos*, Tecnos, Madrid, 1996.

La LORTAD se puede considerar como una de las leyes más protectoras del derecho a la intimidad de los ciudadanos ante los tratamientos informatizados de sus datos personales de todas las existentes en la Unión Europea⁴⁸. Esto se debe en gran parte a que el legislador español tuvo en cuenta los trabajos desarrollados hasta entonces en la Unión Europea para la consecución de la Directiva 95/46.

Por todo esto, la LORTAD ya nació con los principales principios que contendría la regulación comunitaria, si bien se hizo necesaria la reforma tras la aprobación de la Directiva para poder incorporar a nuestro derecho interno los aspectos no incorporados en la misma.

Una vez aprobada la Directiva se hizo necesario modificar la LORTAD, por lo que en principio se pensó en una reforma parcial para lo que el Gobierno remitió al Parlamento un Proyecto de Ley de reforma parcial. Sin embargo en el trámite parlamentario se optó por redactar una nueva ley, que además estableciera un mayor rigor en la protección del derecho a la intimidad de los ciudadanos ante el tratamiento de sus datos personales.

Asimismo, deben tenerse en cuenta, a los efectos de esta materia, el Real Decreto 994/1999, de 11 de junio⁴⁹, que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y el Real Decreto 195/2000, de 11 de febrero⁵⁰, que establece el plazo para implantar las medidas de seguridad previstas por el citado Reglamento.

La problemática del Reglamento reside en su carácter anterior a la nueva LOPD, ya que fue dictado en desarrollo de la derogada LORTAD, por lo que se refiere tan sólo a los datos contenidos en ficheros automatizados, mientras que la reciente LOPD protege los datos registrados en toda clase de soporte, ya se trate de fichero automatizado, microfichas e incluso papel⁵¹.

La nueva LOPD, en vigor desde el 14 de febrero de 2000, ha introducido modificaciones de gran calado, que afectan al conocimiento que de la protección de datos estaba siendo difundido y admitido en general en el Estado español, modificaciones que responden, en gran medida, a la necesaria adaptación de nuestro Derecho a las orientaciones normativas de la Unión Europea y, concretamente, a la Directiva 95/46/CE⁵².

Entre las novedades fundamentales que se presentan⁵³ con la LO 15/99 puede destacarse que:

48 FERNANDEZ LÓPEZ J. M., Conferencia sobre “La regulación del tratamiento automatizado de los datos de carácter personal. El secreto bancario, comunicaciones judiciales y administrativas” pronunciada el 12 de julio de 2000 en el Pazo Mariñán dentro de la Escuela de Verano del Poder Judicial, Bergondo.

49 BOE de 25 de junio de 1999.

50 BOE de 26 de febrero de 2000.

51 AMADOR CONTRA, P., Conferencia sobre “El Reglamento de medidas de seguridad de la Ley de Protección de Datos de carácter personal”, pronunciada el 26 de junio de 2000 en el Auditorio del Edificio FEUGA, Santiago de Compostela.

52 En la Exposición de Motivos del Proyecto de Ley Orgánica por el que se pretendió en principio la modificación de la LORTAD -Proyecto de Ley Orgánica 121/000135, por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, publicado en el *Boletín Oficial de las Cortes Generales*, del 31 de agosto de 1999, Serie A, número 1351-, se indicaban determinadas cuestiones que, con una argumentación ciertamente sencilla, justificaban y argumentaban su modificación, en la necesaria adecuación del Ordenamiento español a la Directiva europea; así, se indicaba expresamente que “tiene por objeto la adaptación...”, que se “procede a introducir en la normativa española reguladora de la materia las modificaciones que vienen reclamadas por el contenido de la Directiva”, o que es necesario únicamente “introducir en aquélla (la LORTAD) las precisas reformas que den como resultado la total adecuación entre dicha Ley y la Directiva comunitaria”.

53 FERNÁNDEZ LÓPEZ, J. M., *Ibidem*.

- se incluyen todos los ficheros de datos, estén o no informatizados. Si bien se difiere respecto a estos últimos la protección hasta el año 2007, sin perjuicio que desde la entrada en vigor de la Directiva los ciudadanos puedan ejercitar sus derechos de acceso, rectificación y cancelación respecto de los datos contenidos en estos ficheros manuales.

- el derecho a la información previa a la recogida de datos ahora se extiende a que en todos los casos se informe al afectado de la existencia del fichero, de la finalidad de la recogida de los datos y de los destinatarios de la información, además de la identidad y dirección del responsable.

- se refuerza la importancia del consentimiento de los ciudadanos para que sus datos puedan ser tratados, exigiéndose que sea: libre, inequívoco, específico e informado. Si bien se exceptúa la necesidad del consentimiento para recabar datos respecto a las fuentes accesibles al público: censo promocional, repertorios telefónicos, listados de profesionales, diarios y boletines oficiales y medios de comunicación.

- respecto a la finalidad para la que pueden tratarse los datos se exige además de que sea legítima, que sea determinada y explícita.

- se incorpora el derecho de oposición con lo que el tratamiento de datos puede evitarse por no llegar a producirse.

- se establecen en el artículo 13 el derecho a no verse sometido a una decisión con efectos jurídicos que se base únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad; así como el derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento; además del derecho a que la valoración del comportamiento sólo pueda tener valor probatorio a petición del afectado.

- en el ámbito sancionador se incorpora la posibilidad de posibilitar la rebaja económica de las sanciones excepcionalmente cuando se aprecie una cualificada disminución del imputado o de la antijuridicidad del hecho.

No obstante, hay que significar que los principios de la protección de datos y los derechos que, mediante su ejercicio, hacen efectiva, o abren el camino para hacer efectiva, la protección, poco o nada cambian, en cuanto a su verdadero contenido, en el texto de la nueva Ley, siendo los mismos, en gran parte, que los recogidos en la LORTAD. Ambos textos -el de la LORTAD y el de la nueva LOPD- responden al contenido del Convenio 108, remarcado básicamente por la referida Directiva.

Las definiciones utilizadas por el articulado se ven ampliadas por varios conceptos terminológicos en el nuevo texto legal, algunos de ellos como exigencia directa de la Directiva cuya transposición se pretende, como puede ser la introducción de la figura del “encargado del tratamiento”, que la experiencia acumulada sostenía que era necesaria en un sector en el que el tratamiento acostumbra a ser, en gran parte de los casos, realizada por un tercero distinto del responsable del fichero.

Igualmente, la introducción en las definiciones del concepto de “fuentes accesibles al público”⁵⁴, estableciendo qué fuentes tienen “exclusivamente” tal consideración, era totalmente necesaria.

54. Sobre el principio de publicidad de las actuaciones judiciales y el acceso, o no, de “cualquier interesado” a los libros, archivos y registros judiciales que no tengan carácter reservado, la sentencia de la Sala 3ª del Tribunal Supremo, de 3 de marzo de 1995, entiende que se debe tener un interés legítimo y relacionado concretamente con el propio objeto del procedimiento o alguno de los actos del mismo.

Por otra parte, el Título II de la LOPD, conservando el epígrafe de “Principios de la Protección de Datos”, mantiene, como señala M. A. DAVARA RODRÍGUEZ⁵⁵, “los principios que permanecen en el tiempo, en múltiples normativas, como base de protección sólida y consolidada interpretativamente”.

Las modificaciones en la redacción de este texto legislativo proporcionarán una nueva visión. Tal es el caso de la obligación de informar cuando los datos no hayan sido recabados por el propio interesado, dentro de los tres meses siguientes a su registro (artículo 5.4 LOPD), lo que supone una sustancial reforma en el principio de información al interesado, obligada por las exigencias contenidas en el artículo 11 de la Directiva.

Igualmente, el artículo 5.5 de la LOPD contempla la posibilidad de que la información al interesado resulte ciertamente imposible o exija esfuerzos desproporcionados, estableciendo la garantía de que todo ello será “a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias”.

En este sentido, la derogada LORTAD preveía en su artículo 40.1 que determinadas competencias podrían ser ejercidas por los órganos correspondientes de las Comunidades Autónomas, a los que se garantizaría plena independencia y objetividad en el ejercicio de su cometido⁵⁶. La nueva LOPD contempla también dichas competencias en su artículo 40.1.

Sin entrar en un análisis sistemático y exhaustivo de la LOPD y de sus novedades con respecto a la LORTAD, lo que por su amplitud y desarrollo precisaría de una mayor reflexión, quedando fuera del ámbito de esta intervención, sí quiero reseñar que el nuevo texto legal ya ha sido objeto de críticas, tanto por parte de la doctrina como de la jurisprudencia española, que ven en su redacción claras imprecisiones terminológicas y de contenido. Fiel reflejo de ello es el Recurso de inconstitucionalidad núm. 1463/2000⁵⁷, promovido por el Defensor del Pueblo, contra determinados preceptos de la LOPD, que el Tribunal Constitucional ha admitido a trámite, por providencia de 28 de marzo del presente año.

No obstante, y en todo caso, pese a que la LOPD necesitará de múltiples estudios y foros para encontrar una línea interpretativa homogénea, debe darse la bienvenida a la Ley que traspone al fin la Directiva, desear que la misma nos sirva a los españoles como instrumento útil para mejor proteger nuestras libertades públicas y derechos fundamentales en lo que concierne al tratamiento de datos personales, así como aspirar a que todos nos concienciamos de la necesidad de su cumplimiento.

Para ello se necesitará de una gran comprensión por parte de todos los implicados, afectados y titulares de ficheros, para poder en la práctica defender y respetar los principios que contiene sin afectar, en lo más mínimo, a una siempre necesaria seguridad jurídica, centrada, como no podía ser de otro modo, en el bien jurídico que se pretende proteger.

55 DAVARA RODRÍGUEZ, M. A., “Los principios de la protección de datos y los derechos de las personas en la nueva Ley Orgánica de Protección de Datos de Carácter Personal” en *Actualidad Informática Aranzadi*, editorial Aranzadi, núm. 34, enero de 2000, Madrid, página 5.

56 Así, por ejemplo, la Agencia de Protección de Datos de la Comunidad de Madrid se crea en la Ley 13/1995, de 21 de abril, de Regulación del Uso de Informática en el Tratamiento de Datos Personales por la Comunidad de Madrid, Ley que fue modificada por iniciativa de la Consejería de Hacienda el 16 de junio de 1997, para facilitar la puesta en marcha de la Agencia.

57 BOE de 8 de abril de 2000.

EL ESPECÍFICO DEL TRATAMIENTO DE DATOS PERSONALES EN LAS RELACIONES BANCO-CLIENTE⁵⁸

* CONSENTIMIENTO EN RELACIÓN CON LA FINALIDAD.

El consentimiento para incorporar a un fichero datos y tratarlos vendrá dado por la firma del contrato del cliente con la entidad; viéndose circunscrito a las finalidades explícitas y legítimas para las que se hayan obtenido. Por lo que el Banco sólo podrá tratar los datos para dar cumplimiento al contrato suscrito con su cliente no pudiendo considerar extensión del mismo fuera del marco contractual establecido.

* OTROS TRATAMIENTOS MÁS COMUNES EN LA PRÁCTICA

Es especialmente conflictivo el tema de las nuevas técnicas de marketing para la obtención de perfiles mediante el “data ware house”, “data mining” o “scoring”. Pues bien, estas técnicas de marketing que posibilitan un conocimiento exhaustivo de las personas y de sus compartamientos suponen un paso más en la invasión de la intimidad, y sólo podrán resultar lícitos cuando previamente se haya informado previamente al ciudadano y éste consienta en ello.

* EJERCICIO DE LOS DERECHOS QUE CORRESPONDEN AL CIUDADANO

La comprobación de la legalidad de los datos que trate la Entidad viene posibilitada por el ejercicio por los ciudadanos de los derechos de acceso, rectificación y cancelación. El derecho de acceso debe permitirse de forma gratuita y extenderse a los datos sometidos a tratamiento, a su origen y a las posibles comunicaciones realizadas; si bien se limita el ejercicio de estos derechos a intervalos no inferiores a 12 meses, salvo que se acredite un interés legítimo al respecto.

* CESIONES DE DATOS MÁS FRECUENTES EN EL SECTOR

Se limita la comunicación a fines directamente relacionados con las funciones legítimas de cedente y cesionario, y se sanciona con nulidad el consentimiento que se obtuvo sin proporcionar la información que permita conocer al interesado la finalidad a la que se destinarán los datos cedidos o el tipo de actividad de aquél a quien se pretenden comunicar.

Si bien se establecen una serie de excepciones a la necesidad de consentimiento para la cesión como cuando la misma esté autorizada por una ley o cuando el tratamiento responda a la aceptación de una relación jurídica cuyo desarrollo o cumplimiento implique una comunicación de datos a tercero.

* EL DEBER DE SECRETO -SECRETO BANCARIO:

Se establece que tanto el responsable del fichero como quienes intervengan en cualquier fase del tratamiento están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizada su relación con el titular del fichero.

En el ámbito específico de las entidades financieras el deber de guardar secreto tiene una amplia tradición que excede del secreto que se exige con carácter general. Si bien se va limitando paulatinamente con la Ley General Tributaria, Ley 26/1988 sobre Disciplina e Intervención de las Entidades de crédito, la Ley 13/1994 de Autonomía del Banco de España, y muy especialmente por la Ley 19/1993 sobre determinadas medidas de prevención del blanqueo de capitales.

58 FERNÁNDEZ LÓPEZ, J.M., *Ibidem*.

En definitiva el secreto bancario vendrá justificado por la protección del derecho a la intimidad y este derecho con el resto de los fundamentales tiene su límite en los restantes y ante la colisión de dos o varios de ellos deberá prevalecer, dependiendo de los supuestos, aquel en que el bien jurídico protegido deba de primar atendiendo al caso concreto.

* COMUNICACIONES JUDICIALES Y ADMINISTRATIVAS

- Comunicaciones judiciales:

El deber genérico de contar con el consentimiento previo del interesado para ceder o comunicar datos a un tercero, cede en los supuestos en que la comunicación tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal o Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidos.

En la LOPJ se establece que los Jueces y Tribunales pueden utilizar cualquier medio técnico informático o telemático para el ejercicio de sus funciones con las limitaciones previstas por la legislación sobre protección de datos, correspondiendo al CGPJ la aprobación de un reglamento de los requisitos para la gestión de los ficheros, lo que se hizo con el Reglamento 5/1995 de 7 de junio.

En él se distinguen entre ficheros jurisdiccionales y no jurisdiccionales; según se formen con datos de carácter personal que figuren en los procesos de los que conozcan y los segundos con los datos de carácter personal que consten en los procedimientos gubernativos.

En los ficheros jurisdiccionales solamente se contendrán datos de carácter personal que deriven de las actuaciones jurisdiccionales y, en particular los que sean necesarios para el registro e identificación del procedimiento; los necesarios para la identificación y localización de quienes puedan tener derecho a intervenir como parte; los necesarios para la identificación de quienes asuman las labores de defensa o representación procesal o que intervengan en cualquier otra calidad en el procedimiento o asunto; los que exterioricen las resoluciones dictadas y las actuaciones en él realizadas y los derivados de la instrucción o tramitación de las diligencias judiciales.(art 78.2).

Los datos serán conservados en tanto su supresión no sea ordenada por decisión judicial, o se produzca su caducidad informática.

- Comunicaciones administrativas

La LOPD exige que la cesión de datos personales se realice con el consentimiento del afectado, salvo en los casos contemplados en el art. 11.2. La cesión sólo será lícita si se dan acumulativamente dos condiciones: que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario (lo que exige que los datos tratados sean pertinentes, proporcionados y oportunos para el fin que se pretende conseguir), y que se cuente con el consentimiento previo del interesado.

Los ficheros automatizados de la Administración tributaria y de la Seguridad Social disponen de un contenido de gran riqueza y volumen que incluyen datos de carácter personal sobre millones de ciudadanos, por lo que merecen un estudio singularidad.

+ Ficheros de la Administración tributaria:

Las cesiones de datos personales por parte de las entidades financieras a la Hacienda afecta principalmente a las de sus clientes en virtud del deber de colaboración que impone la Ley General Tributaria. El artículo 112.4 de la LGT (modificado por la disposición adicional cuarta de la LOPD) establece una excepción en la regla general

del consentimiento previo del afectado, y así las entidades financieras pueden estar obligadas a ceder a la Hacienda toda clase de datos de trascendencia tributaria deducidos de sus relaciones económicas, personales o financieras con sus clientes.

La cesión de datos a la Hacienda Pública es tan amplia que incluso no se le aplica la prohibición de comunicación a otras Administraciones Públicas de datos recabados para competencias diferentes (art. 21.1 LOPD).

Este régimen singular de los ficheros tributarios responde a la obligación de la Hacienda Pública de velar por el cumplimiento del deber, impuesto por nuestra Constitución en su artículo 31.1, de todos los ciudadanos de contribuir al sostenimiento de los gastos públicos de acuerdo con su capacidad económica.

+ Ficheros de la Seguridad Social

El apartado 7º del artículo 36 del Real Decreto Legislativo 1/1994, de 20 de junio, por el que aprueba el Texto Refundido de la Ley de la Seguridad Social, los regula de una forma análoga a la de los ficheros de la Seguridad Social.

* LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN INTERNET

La creciente importancia que la red "Internet" tiene en España, tanto para los ciudadanos como para el tejido empresarial y, por tanto, para el conjunto de la sociedad, hace imprescindible el establecimiento de un marco estable para la gestión del sistema de nombres de dominio⁵⁹.

Las normas básicas de nuestro Ordenamiento en materia de protección de los datos personales se proyectan plenamente sobre los servicios de la sociedad de la información, si bien el grave problema es la internacionalización, lo que hace preciso un amplio acuerdo a ese nivel para establecer un adecuado marco jurídico, con sus correspondientes sanciones, que garantice el correcto funcionamiento y utilización de la red internet, con la correspondiente protección de los datos de carácter privado, que deben tutelarse adecuadamente y de manera compatible con el interés empresarial en la recopilación de datos.

La interconexión a nivel mundial de las redes digitales promueve la globalización de la información, de manera que Internet constituye un medio propicio para la circulación transfronteriza de datos, lo que genera riesgos específicos respecto de los datos de carácter personal⁶⁰. Por otra parte Internet también se caracteriza por el empleo de técnicas que incrementan los datos personales susceptibles de quedar bajo control⁶¹.

Estos elementos aconsejan la aproximación al régimen de protección instaurado en nuestro país, con especial acento en el de responsabilidad civil y en el relativo al movimiento internacional de datos, vinculado a la diversidad de niveles de protección existentes a nivel comparado⁶².

59 Resolución de 10 de febrero de 2000 de la Secretaría General de Comunicaciones, publicada en el BOE de 8 de marzo de 2000.

60 GEIS I., "Internet und Datenschutzrecht" en *NJW*, volumen 50, 1997, página 288.

61 RIBAS ALEJANDRO, J., *Aspectos jurídicos del comercio electrónico en Internet*, Pamplona, Aranzadi, 1999, páginas 50 a 52.

62 DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, Civitas, 2000, página 473.

En España, la Orden de 21 de marzo de 2000 regula el sistema de asignación de nombres de dominio de Internet bajo el código de país correspondiente a España (.es)⁶³. Dicha Orden manifiesta que el sistema de nombres de dominio se emplea en Internet para poder utilizar universalmente nombres unívocos para vincularlos a los usuarios de los equipos conectados a la red.

De esta forma, los usuarios pueden emplear nombres en lugar de números, lo cual supone enormes ventajas como una mayor comodidad de utilización, si bien, como es lógico, únicamente tiene alcance nacional, residiendo, como hemos adelantado, el problema en el carácter mundial de la red Internet, de modo que España sólo puede legislar, en los términos vistos, para los nombres bajo el código .es, pero en Estados Unidos se registran en ICANN (*Internet Corporation for Assigned Names and Numbers*).

En efecto, recientemente se ha creado la organización supranacional, de carácter privado, ICANN, la cual asume la responsabilidad de la administración, en el ámbito mundial, de los nombres y direcciones numéricas de Internet, que se registran en Estados Unidos en aplicación del principio en cuya virtud el primero que llega consigue el nombre que quiera (*prior tempore, potior iure*), y todo ello al margen de que es muy probable que en breve haya muy diversos nombres de dominio genéricos, pues dentro del código .com están agrupadas multitud de actividades que ya no caben y se tiende a la especialización.

Ante el vacío jurídico parcial existente en la utilización de la red internet, dado el impacto mundial propio de las actividades en este medio, es imprescindible establecer un amplio acuerdo internacional que regule su adecuado uso, con las correspondientes sanciones, y, de manera particular, evite el posible registro, con fines puramente lucrativos, de dominios ajenos en Internet, y que, tras su correspondiente registro, en un acto de auténtica "piratería", se intenta vender o alquilar a la empresa titular de la marca oficial, como sucedió con la firma británica *Burguer King*, a la que ofrecieron su nombre por 25.000 libras esterlinas, casi siete millones de pesetas, o el caso de una empresa alemana que poseía cerca de 2.000 nombres, entre ellos todas las marcas de automóviles (Ford, Opel, Citroën...), o como ocurrió en España con el nombre Nocilla, sobre el que recayó un auto de un juzgado de primera instancia de Oviedo en junio de 1999.

* REGULACIÓN DE LA FIRMA ELECTRÓNICA EN NUESTRO ORDENAMIENTO

Como es bien sabido, en el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente desaparecen las tradicionales firmas manuscritas que pueden ser reemplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica⁶⁴.

El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica⁶⁵, en su artículo 15 se refiere a la protección de los datos personales en este ámbito. A tenor de este precepto el tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación se sujetan a lo dispuesto en la Ley Orgánica de Protección de Datos.

63 BOE de 30 de marzo de 2000.

64 MARTÍNEZ NADAL, A., "Comentarios de urgencia al urgentemente aprobado Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica (I)" en *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*, número 4939, Madrid, 1999, página 2.

65 BOE de 18 de septiembre de 1999.

El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

En cualquier caso, lo que resulta indudable es que el comercio electrónico constituye, sin lugar a dudas, el futuro de las transacciones económicas en todo el mundo y, como consecuencia, los nombres de dominio han pasado a tener una importante función comercial, resultando posible, en la actualidad, ante el vacío jurídico parcial que existe al respecto, que empresas, en un acto de auténtica "piratería", se dediquen a registrar nombres ajenos y después intenten venderlos o alquilarlos a la empresa titular de la marca oficial.

IV. CONCLUSIONES

1ª Todo sistema de tratamiento de datos personales debe encontrar su fundamentación en el servicio que presta a las personas. Para lograrlo se hace necesario un respeto a las libertades y derechos fundamentales, especialmente al derecho a la intimidad.

2ª La enorme trascendencia de los intereses que confluyen en el tema de la protección de datos personales en el Derecho Comunitario hace necesaria una regulación exhaustiva.

Así, nos encontramos con la necesidad de no entorpecer el desarrollo de las técnicas de telecomunicaciones e información, imprescindibles para la sociedad de nuestros días, lo que se debe conjugar y coherente adecuadamente con los intereses de los Estados, no interesados en ceder excesivamente su soberanía y, fundamentalmente, con los intereses de las personas físicas, puesto que son los principales afectados en la materia, al ser sus datos los que demandan una adecuada regulación.

3ª La aprobación en España de la nueva Ley Orgánica de Protección de Datos, de 13 de diciembre de 1999, responde no sólo a la incorporación de la Directiva 95/46, sino también al establecimiento de un mayor rigor en la protección del derecho a la intimidad de los ciudadanos ante el tratamiento de sus datos personales.

4ª Resulta imprescindible fomentar la formación sobre el conocimiento y aplicación de la legislación de protección de datos para conseguir que la cultura de posesión de datos personales se integre en la vida cotidiana de todos y se garantice la privacidad de datos personales especialmente protegidos, como la ideología, religión o incluso la salud o las infracciones penales o administrativas y tributarias.

5ª El potenciamiento de las tecnologías informáticas que permiten a las comunidades periféricas superar el aislamiento y competir en la economía global, debe ser compatible con el respeto y la defensa de la intimidad y demás derechos personales, siendo necesario un mayor rigor en la protección del derecho a la intimidad.

6ª Resulta necesaria la urgente adopción de adecuadas medidas de garantía y seguridad en la utilización de la red Internet con la implantación de criterios comunes de evaluación de la protección de datos personales que puedan determinarse a escala comunitaria o, incluso, mundial, resultando absolutamente insuficiente, aun cuando es necesaria, la regulación a nivel nacional (que en España se concreta en una Orden de marzo de 2000 del Ministerio de Fomento para el registro de los nombres de dominio en internet) ante el indudable alcance global de este medio y las importantes limitaciones de los distintos Estados para garantizar la efectividad de ciertas sanciones relativas a actividades desarrolladas en internet.

7ª El comercio electrónico constituye el futuro de las transacciones económicas en todo el mundo y, como consecuencia, los nombres de dominio han pasado a tener una importante función comercial, resultando posible, en internet, que empresas, en un acto de auténtica "piratería", se dediquen a registrar nombres ajenos y después intenten venderlos o alquilarlos a la empresa titular de la marca oficial.

Ante el vacío jurídico parcial existente en la utilización de la red Internet, dado el impacto mundial propio de las actividades en este medio, es imprescindible establecer un amplio acuerdo internacional que regule su adecuado uso, con las correspondientes sanciones, y de manera particular el aludido registro, con fines puramente lucrativos, de dominios ajenos en internet, como sucedió con la firma británica Burguer King, a la que ofrecieron su nombre por 25.000 libras esterlinas, casi siete millones de pesetas, o el caso de una empresa alemana que poseía cerca de 2.000 nombres, entre ellos todas las marcas de automóviles (Ford, Opel, Citroën...).

8ª. El éxito en la utilización de las nuevas formas de telecomunicación depende en gran medida de la confianza de los usuarios en que no se ponga en peligro su intimidad, ni se atente contra ella, junto, desde luego, con las necesarias garantías en su funcionamiento correcto, para lo cual resulta un buen paso el Centro de Arbitraje y Mediación de Ginebra, en funcionamiento desde principios de este año.