

LA LIBERTAD INFORMÁTICA
INDICE

1.- Introducción. Objeto del trabajo. El Derecho a la Libertad Informática como límite a la creciente utilización de tratamientos automatizados con datos de carácter personal. Aproximación al concepto.....	1
2.- Primeras menciones del derecho.....	4
-Resolución 509 de 1968 de la Asamblea del Consejo de Europa.....	5
-Guidelines on the Protection of Privacy and Transborder Flows of Personal Data OECD. 23 de septiembre de 1980).....	6
-La Sentencia de 15-12 1983 del Tribunal Federal alemán.....	8
-Acuerdo de Schengen. Importancia del mismo. Relación del Acuerdo de Schengen con el Convenio 108 del Consejo de Europa.....	9
-Principios rectores para la reglamentación de los ficheros automatizados de datos personales (adoptados por la Asamblea General de las Naciones Unidas en su resolución 45/95 del 14 de diciembre de 1990).....	10
3.- Convenio 108 del Consejo de Europa: importancia del mismo. Principios rectores y definiciones básicas. El alcance normativo en España según la Sentencia 254/93, del Tribunal Constitucional.....	11
4.- La Ley 5/92, Reguladora del Tratamiento Automatizado de Datos (LORTAD).....	13
5.- -La Directiva 1995/46/CE, del Parlamento 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.....	15
6.- La Ley 15/99, de Protección de Datos de Carácter Personal. (LOPD).....	17
7.- Interpretación del Tribunal Constitucional:	
-Sentencias 209/88, 231/88, 223/92: una aproximación al concepto de intimidad según el Tribunal Constitucional.....	21
-Sentencia 53/1985: el Estado ha de tener una postura activa en la protección de los derechos fundamentales recogidos en la Constitución. Estos derechos recogen también facultades positivas para el individuo.....	22
-Sentencia 254/93, 290/2000 y 292/2000: la doble vertiente de la libertad informática. Los límites de este nuevo derecho.....	22
-Sentencia 143/94: el principio de finalidad en la recogida de datos.....	26
-Sentencia 11/98, 60/98 y 94/98: utilización de datos para finalidades no permitidas. Los datos especialmente protegidos. La justificación de la protección para esta clase de datos.....	27
-Sentencia 202/99: necesidad del consentimiento expreso para tratar datos especialmente protegidos.....	28
8.- Conclusión.....	30

LA LIBERTAD INFORMÁTICA

1.- Introducción. Objeto del trabajo. El Derecho a la Libertad Informática como límite a la creciente utilización de tratamientos automatizados con datos de carácter personal. Aproximación al concepto.

Resulta innegable que la aparición de las “TIC” como herramienta potenciadora de la actividad empresarial, trae consigo una variedad de problemas jurídicos de diversa índole. Entre éstos, los más relevantes se presentan como aquellos que hacen referencia a derechos constitucionalmente reconocidos, y más concretamente, los relativos a la privacidad de los usuarios o interesados. En efecto: con frecuencia encontramos en la prensa diaria noticias sobre la aparición de historiales clínicos en la calle, o cesiones de datos considerados como especialmente sensibles sin el previo consentimiento expreso. Resulta lamentable, pero, esto es mucho más habitual de lo que en un primer momento pudiera parecer¹.

Pero nuestros tribunales y legisladores han actuado activamente, y han arbitrado una serie de sentencias y disposiciones que favorecen en la mayoría de los casos derechos que, como se mencionaba antes, están constitucionalmente reconocidos. Lo cierto es que estas disposiciones no son precisamente nuevas en el tiempo, y en algunos casos hay que remontarse a la década de los 70 u 80 para encontrar documentos verdaderamente importantes, donde el esfuerzo previsor era patente².

En otras ocasiones, han sido los jueces los que han dictado sentencias innovadoras en relación a estos aspectos. Este conflicto “TIC-Derechos de la personalidad” no tardó en producirse en los tribunales, alcanzándose soluciones favorables al reconocimiento de un nuevo derecho, el de “autodeterminación informativa”³, en algunas de ellas.

El objeto del presente trabajo monográfico es dar una visión general de este derecho reconocido en nuestros tribunales, valiéndonos para ello de las principales disposiciones, sentencias y en definitiva, resoluciones importantes que hagan referencia a esta materia.

¹ Como señalan los autores, “...la tecnología informática permite (gracias a sus posibilidades prácticamente ilimitadas de captar, almacenar, relacionar y transmitir todo tipo de datos) reunir de forma personalizada, a partir de informaciones dispersas –e incluso anónimas-, múltiples facetas de la vida de hombres y mujeres totalmente ajenos al hecho de que sus hábitos vitales están en manos de terceros dispuestos a utilizarlos y aun a costa de depararles perjuicios importantes...” *“Utilización y control de datos laborales automatizados”*, Juan José Fernández Domínguez y Susana Rodríguez Escanciano. Agencia de Protección de Datos. 2001. Pág. 1

² Desde luego es encomiable que nuestros constituyentes (sin duda, el ejemplo más relevante) tuvieran la “visión de futuro” de prever, en el año 1978, que las TIC podrían poner en peligro derechos como los referentes al honor, intimidad y propia imagen. Fruto de ello es la redacción del art. 18.4.

³ Stc 254/93 del Tribunal Constitucional o más recientemente, 290/2000, por citar sólo dos ejemplos.

Si bien es cierto que en nuestro país existen multitud trabajos doctrinales que hacen referencia al “derecho a la intimidad” tanto en la vertiente penal o civil del mismo, no encontramos tantos estudios que profundicen en el derecho a la “autodeterminación informativa” configurándolo como un derecho “autónomo e independiente”, como ha señalado nuestro Tribunal Constitucional en reiteradas ocasiones⁴. Apenas se discute la existencia del mismo. Entre los mayores defensores se encuentran los profesores Lucas Murillo de la Cueva y Manuel Heredero Higuera. El argumento principal que encontramos para ello descansa sobre la siguiente afirmación: si se pretendía una sola tutela de los derechos recogidos expresamente en el art. 18 de la Constitución, hubiera bastado con leyes como la Ley Orgánica 1/1982⁵, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y con la Ley Orgánica 7/1984, de 15 de octubre, de tipificación penal de las escuchas telefónicas.

Como ha señalado en reiteradas ocasiones el actual director de la Agencia de Protección de Datos de la Comunidad de Madrid, D. Antonio Troncoso, llama la atención que la única vez que la Constitución se refiere a la informática sea para limitar su uso. Se trata de que un elemento provechoso no sea utilizado para recortar la privacidad de las personas⁶. Sin embargo, ha sido necesaria una construcción de nuestro Tribunal Constitucional, vertebrada principalmente a raíz de la Sentencia 254/93, para ir delimitando las fronteras de este nuevo derecho. Para algunos autores⁷, nuestra Carta Magna no tutela expresamente la libertad informática y es necesaria esa construcción jurisprudencial a la que hemos aludido. Lo cierto es que hoy en día sí contamos con esa jurisprudencia, siendo el objeto principal del trabajo el aludir a la misma para intentar dibujar esos límites.

⁴ En este punto es necesario mencionar al profesor Antonio Enrique Pérez Luño como artífice de la introducción en España de la expresión «derecho a la autodeterminación informativa».

⁵ Precisamente se establece en la Disposición Transitoria Primera de esta Ley que “en tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuarto de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley.”

⁶ “Es una respuesta constitucional ante una amenaza concreta”. Antonio Troncoso Reigada. *Manual práctico de Protección de Datos para las Administraciones Públicas*. Civitas, 2004.

⁷ Véase el excelente artículo de Rafael Allende Mendizábal, *“La libertad Informática, un novísimo derecho fundamental”*, publicado por la Agencia de Protección de Datos. Para este autor, una de las tareas fundamentales de los Tribunales Constitucionales es extender la tutela de determinadas áreas – como la libertad informática- no expresamente reconocidas en los textos constitucionales, y aplicarlas a determinados supuestos de la vida cotidiana de los ciudadanos. No proceder con esa tutela significaría dejar “vacías” ciertas áreas que reclaman pronunciamientos en uno u otro sentido: “lo que quiere subrayarse es que la Constitución incluye un catálogo inacabado, que ha de ser completado si otros derechos reclaman, con exigencias razonables, la tutela constitucional”. En la actualidad, en el ámbito de la Constitución Europea, tras debatir varias propuestas planteadas en el Grupo Carta se decide incluir en la Parte I del texto constitucional de forma expresa e independiente del resto de los derechos de la Carta el derecho a la protección de datos.

Estamos ante un nuevo derecho, no siendo suficiente la clásica mención al Honor, Intimidad y Propia Imagen de nuestro Tribunal Constitucional para referirnos al mismo⁸. Podemos definirlo como el derecho al control sobre los datos relativos a la propia persona insertos en un Sistema de Información que faculta al interesado para decidir quién posee esos datos, y para qué los va a usar, pudiendo oponerse a ello si lo estima conveniente⁹. Este derecho ha de sustanciarse confiriendo al interesado un haz de facultades que deberá esgrimir ante aquella entidad que esté tratando información relativa a su persona, pero también faculta a su titular para oponerse a determinados comportamientos.¹⁰

2.- Primeras menciones del derecho.

Es claro que la protección de datos ha ido variando desde una primera etapa, que podríamos situar en la década de los 60¹¹, donde la informática apenas tenía importancia en el tejido empresarial de los países, hasta la actualidad, donde las grandes megabases de datos son cruzadas, unas con otras, para obtener perfiles de la personalidad del individuo, donde cantidades ingentes de información son transmitidas por redes públicas de telecomunicaciones, y donde la potencia de los procesadores ha crecido exponencialmente.¹² Es igualmente evidente que ha habido una evolución en las normas reguladoras de esta materia, siendo sin lugar a dudas un aspecto mucho más trascendental en la actualidad que lo que lo fue en sus auspicios. Y por supuesto, las circunstancias, eran distintas¹³.

⁸ Establece la Sentencia 231/98 del Tribunal Constitucional: “Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la C.E. aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona», que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo.”

⁹ Señala Pérez Luño: «aparece como un *nuevo derecho* de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en las tarjetas de un programa electrónico». Segundas Jornadas de Abogacía e Informática. Ilustre Colegio de Abogados de Barcelona.

¹⁰ Por ejemplo, la oposición del titular de los datos a que los mismos sean tratados durante mas tiempo del estrictamente necesario. O a ser informado en el momento de la recogida.

¹¹ A pesar de que la era de la informática la situaremos justo después de la II Guerra Mundial como señala D. Emilio Suñé Llinás, en su obra “Tratado de Derecho Informático”: “Al entrar en la era de la informática, cosa que sucederá inmediatamente después de la Segunda Guerra Mundial, el ser humano se vuelve más y más de cristal, a partir del tratamiento masivo de los más diversos datos de las múltiples acciones de su vida cotidiana, que son susceptibles de quedar, y de hecho quedan, registrados en un ordenador.”

¹² Por ejemplo, dos supuestos muy concretos que forman parte de los tratamientos automatizados de datos que se realizan en la actualidad son el “data mining” o “data warehouse”. Se trata de herramientas utilizadas para la toma de decisiones en los campos comercial y de marketing. Era imposible, dada la potencia de los procesadores, que existieran estas herramientas en décadas anteriores a la de los 80.

¹³ Para María de los Reyes Corripio Gil Delgado, “No se trata sólo de la elaboración de bancos de datos relativos al comportamiento de las personas, sino el tratamiento posterior que se hace de ellos, como su transferencia a terceros o su utilización para el mercadeo de productos no solicitados. La tecnología

El profesor Pérez Luño habla de distintas generaciones en las leyes de protección de datos, que se correspondería con una evolución de la informática y de la tutela de la intimidad. En una primera generación, que estaría basada en la autorización previa de los bancos de datos, los equipos informáticos eran escasos, voluminosos en su tamaño y de potencia computacional limitada. Una segunda generación tuvo el objetivo de garantizar los datos “sensibles”, en la inteligencia de que era necesario proteger una cierta tipología de información referente a los individuos que podría suponer un daño mayor a su intimidad que el resto de informaciones sobre su persona. La tercera generación, en la que nos encontramos, se caracteriza por la aparición de la microinformática y por la “difusión” de las informaciones con carácter personal. Si antes se necesitaba una máquina que ocupaba dos manzanas y media de edificios, ahora bastan unos cuantos centímetros.¹⁴

Sin duda, la normativa ha ido evolucionando y acogiendo nuevos principios y excepciones. Parece por tanto necesario ver cómo se ha producido esta evolución, atendiendo a un criterio cronológico.

Resolución 509 de 1968 de la Asamblea del Consejo de Europa.

Se destaca esta Resolución por ser la primera en la que se alude a las Tecnologías de la Información no sólo como una herramienta innovadora, sino también como una posible “arma de doble filo” si no se ponen límites a ella.

A partir del año 1968 la actividad del Consejo de Europa en este sentido fue bastante prolífica. Caben destacar las siguientes iniciativas:

- En el año 1971 el Comité de Ministros designa una comisión de expertos, encargada de elaborar proyectos para la tutela de las libertades, en especial del derecho a la intimidad, frente a los avances tecnológicos.
- Resolución del Comité de Ministros de 26 de Septiembre de 1973, relativa a "La protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado".

digital permite aplicar técnicas de publicidad one to one mucho más agresivas y baratas que los tradicionales medios de comunicación como el teléfono o la correspondencia”. *“La regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet”*. Agencia de Protección de Datos. 2001.

¹⁴ El ejemplo no es gratuito. En 1946 se diseñó el ENIAC (Electronic Numerical Integrator and Calculator), con 18.000 válvulas electrónicas. En la actualidad, las PDAs son las reinas del mercado, pudiendo realizar operaciones muy complejas.

- Resolución de 20 de Septiembre de 1974 relativa a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público".
- Resolución del Comité de Ministros de 1976 por la que se crea una comisión de expertos encargada de desarrollar los trabajos preparatorios de lo que será un futuro Convenio sobre la materia

A pesar de que en esta Resolución no se alude a la Protección de Datos como tal, si se hace eco de la peligrosidad que las aún incipientes Tecnologías de la Información podrían tener sobre la persona. La preocupación del Consejo de Europa puede considerarse pionera en el ámbito de las organizaciones internacionales.

Así, en el año 1967, se creó una comisión consultiva para estudiar el impacto de las nuevas tecnologías en el ámbito de los Derechos Humanos. Un año después, esa comisión redactó la citada Resolución, donde se revela la necesidad de establecer mecanismos de protección tanto sobre la vida privada de las personas como sobre otros derechos fundamentales que podrían afectarse con la aparición de las nuevas tecnologías.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 23 de septiembre de 1980).

Las razones que impulsaron a la Organización para la Cooperación y el Desarrollo Económicos (OCDE) a redactar un texto en sintonía con los trabajos que el Consejo de Europa estaba ya realizando y que daría su fruto tan sólo un año después, fueron prácticamente las mismas que las mencionadas en el anterior punto: la creciente importancia de las redes de telecomunicaciones, la aparición de la informática como un elemento imprescindible en la actividad empresarial además del uso que se hacía de la misma en el sector público, siempre en relación con la información de carácter personal tratada.

De una primera lectura del documento, llama la atención la coincidencia de muchos de los conceptos con los contenidos en el Convenio 108 del Consejo de Europa.¹⁵ Así “datos personales” son considerados “cualquier información relacionada con un individuo identificado o identificable” y “flujo transfronterizo de datos personales” se correspondería con el concepto de “movimiento internacional de datos”, al ser definida como “el movimiento de datos personales a través de fronteras nacionales”. Esta coincidencia también lo es respecto de los principios: “Principio de limitación de la recogida” –los datos han de recogerse con el

¹⁵ Y, por extensión, la mayoría de los conceptos y principios del Convenio 108 han sido y son los coincidentes con las leyes 5/92 y 15/99, actualmente en vigor.

consentimiento del interesado, y con medios legales y justos- el conocido “Principio de Calidad de los Datos” –respeto a la finalidad para la cual fueron recabados, necesidad de que los mismos sean exactos, completos, actuales y necesidad de que sean eliminados cuando la finalidad desaparezca, a no ser que existan leyes donde se especifique otra cosa- o el “Principio de Salvaguardía de la Seguridad”¹⁶, donde se alude a la necesidad para el Responsable del Fichero de establecer las medidas organizativas y técnicas que garanticen la seguridad de los datos de carácter personal.

Como se establece en el propio resumen del documento, “las directrices de privacidad suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal. Los principios establecidos en las directrices de privacidad se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos. Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado). Los principios se pueden aplicar en los ámbitos nacional e internacional. A lo largo de los años se han utilizado en gran número de instrumentos de regulación nacional o de autorregulación y todavía se usan ampliamente en los sectores público y privado”. Es este afán “universal” y “con un marcado carácter generalista” quizás lo más destacable. Los principios y los conceptos buscan ser aplicados en todos los sectores y en todos los ámbitos. Se trata de un documento que influiría claramente en el Convenio 108.

La Sentencia de 15-12 1983 del Tribunal Federal alemán

Estamos ante la confirmación definitiva de la existencia del derecho a la libertad informática. Es preciso destacar que en la Constitución Alemana¹⁷ no se recoge ninguna mención expresa a la informática, como si ocurre en la Constitución Española. Además, tampoco se recoge mención expresa alguna al derecho a la intimidad. Los jueces tuvieron que acudir por tanto al derecho al libre desarrollo a la personalidad, reconocido como derecho fundamental.

¹⁶ Principio que se corresponde con el art. 9 de nuestra Ley 15/99. En la actualidad, el Real Decreto 994/1999 es el texto al cual es necesario remitirse para establecer esas medidas de seguridad. Real Decreto que, aunque referido a la ya derogada Ley 5/92, se ha mantenido expresamente vigente.

¹⁷ *Grundgesetz* o Ley Fundamental alemana.

La sentencia establece con argumentos muy claros el peligro que supone la recogida excesiva e injustificada de datos de los ciudadanos por la administración. Y declara sin lugar a dudas que la “autodeterminación del individuo”, o “el derecho a tomar las decisiones que el mismo crea convenientes” puede verse coartado si conoce o sabe que ciertos poderes públicos tienen informaciones referentes a su persona. La conexión es clara: si el ciudadano sabe que en una reunión pacífica se van a grabar las conversaciones, muy probablemente este individuo se vea coartado en sus manifestaciones. Es esta autodeterminación del individuo la que está en juego, que se pone en peligro si al mismo se le piden excesivas informaciones –datos, en definitiva- sin justificación aparente. De la misma forma, parece excesiva y atentatoria contra esta autodeterminación la recogida injustificada de informaciones referentes al “último puesto que ocupó en una empresa” o “fuente de los medios principales de subsistencia”.

Pero en algunos casos, la recogida de informaciones si está justificada. Son aquellos en los que prevalezca un interés general, y exista un mandato constitucional. No parece que la Ley del Censo alemana cumpla estos requisitos. Además, en la sentencia se establece que en todo caso el legislador debe implantar “medidas de derecho procesal” y de “índole organizativa” susceptibles de contrarrestar la posición del individuo o interesado.

La Sentencia concluye que ciertas informaciones que se pretende recoger “contravienen el derecho general de la personalidad”. Pero hay otras que no, las recogidas en el artículo 9 párrafo 4º, utilizadas para fines científicos. En todo caso han de respetarse ciertas garantías.¹⁸

Es claro que en cantidad de ocasiones, las finalidades utilizadas para la recogida de datos se desvían. Los datos recogidos para fines demográficos o científicos suelen ser muy apetecibles para elaborar conductas de la personalidad. Es por ello que las garantías deben de prevalecer en todo momento ya que el “Principio de la Finalidad de los Datos”, hoy reconocido en nuestra Ley 15/99, se puede vulnerar muy fácilmente¹⁹.

Se puede decir después de esta sentencia que existe un concepto “positivo” del derecho a la intimidad, cuando antes se consideraba nada mas que su esfera “negativa”. Y ello porque se

¹⁸ «la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de datos concernientes a la persona. (...) El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales». Sentencia del Tribunal Federal Alemán de 15 de Diciembre de 1983.

¹⁹ En la Segunda Guerra Mundial, Hitler hizo uso de la ley del censo para identificar a la población judía. El ejemplo es bastante elocuente de lo que puede llegar a ocurrir si existe este desvío de la finalidad.

deben arbitrar algunas medidas directas de cara al individuo para que el mismo controle el flujo de datos personales existentes.

Acuerdo de Schengen. Importancia del mismo. Relación del Acuerdo de Schengen con el Convenio 108 del Consejo de Europa.

Se trata de un acuerdo relativo a la suspensión gradual de los controles en las fronteras comunes. Los objetivos del mismo tienen que ver con la colaboración en la extradición, asistencia judicial en materia penal, aplicación del principio non bis in idem y efectividad de las sentencias penales.

Pero se necesitaba una infraestructura tecnológica. El acuerdo contemplaba en el Título IV la creación de un sistema de información común de carácter policial, el “SIS”, Sistema de Información de Schengen. Se intentan establecer una serie de límites a la información que puede tratar este sistema, estableciendo que “el Sistema de Información de Schengen incluye exclusivamente las categorías de datos que proporciona cada una de las Partes contratantes y que son necesarias para los fines previstos en los artículos 95 a 100”. Por otro lado, se establece un amplio catálogo de datos que pueden ser procesados: nombre, apellidos, fecha, sexo, nacionalidad o conducta que debe observarse.

El Acuerdo de Schengen fue establecido el 14 de Junio de 1985 entre el Benelux, la República Federal Alemana y Francia. Al mismo se adhirió posteriormente España, Portugal y Grecia. España lo hizo el 25 de Junio de 1991 y se ratificó el 23 de Julio de 1993.

Una pieza imprescindible para que todo el sistema funcione es el grado de veracidad de los datos que cada país aporta. Se establece que cada nación será responsable de los datos aportados. Y para conseguir esto, se estableció que los países firmantes han de adoptar las disposiciones necesarias que garanticen un nivel de protección de los datos de carácter personal que sea al menos, igual al resultante de los principios del Convenio del Consejo de Europa de 28 de Enero de 1981 para la protección de las personas en lo referente al tratamiento automatizado de datos de carácter personal y respetando la Recomendación R(87)15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía (art. 117 del Convenio). En suma, adoptar el Convenio de Schengen significaba que España debía respetar los principios del

Convenio 108, y la mejor forma de hacerlo era legislando. La LORTAD no se haría de esperar demasiado.²⁰

Como fruto de este compromiso, podemos decir que se aceleró el mandato constitucional recogido en el art. 18.4, posibilitando la creación de la Ley 5/92, Reguladora del Tratamiento Automatizado de Datos. No obstante, incluso antes de la entrada en vigor de esta ley, otros textos se modificaron buscando el respeto a los principios del Convenio 108.²¹

Principios rectores para la reglamentación de los ficheros automatizados de datos personales (adoptados por la Asamblea General de las Naciones Unidas en su resolución 45/95 del 14 de diciembre de 1990).

Son una serie de orientaciones para los estados que pretenden legislar sobre la materia. Se establecen una serie de principios que han de venir recogidos en las leyes correspondientes. Entre ellos, se destaca:

1. Principio de la licitud y lealtad: Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud: Las personas encargadas de la creación de un fichero o de su funcionamiento deberán tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando

Se recogen otros principios como el de “Principio de acceso de la persona interesada”²², el “Principio de no discriminación” o, por supuesto, el “Principio de finalidad”. La mayoría de

²⁰ Como señala Emilio Del Peso Navarro en su obra “*Lortad, reglamento de seguridad*”, “en unos momentos en que el Gobierno de España quería figurar en todas las instituciones europeas, la falta de una ley de protección de datos de carácter personal era un obstáculo para formar parte del Grupo Schengen y para lograrlo de forma un tanto rápida se procede a su publicación después de un gran intervalo de tiempo, desde la aprobación del mandato constitucional del art. 18.4, sin hacerlo”.

²¹ Por citar sólo unos ejemplos, se modifica la Ley General Tributaria por leyes 10/85 y 4/90, la Ley 30/84, de medidas para la Reforma de la Función Pública o la Ley 19/88, de Auditoría de Cuentas.

²² Dispone este principio que “toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios”. En la actualidad, estos otros derechos –acceso, cancelación, oposición y rectificación– están recogidos en nuestra Ley 15/99 y desarrollada por la Instrucción 1/98 de la Agencia de Protección de Datos.

estos conceptos se corresponden con los contenidos en el Convenio 108 o en el texto de la Organización para la Cooperación y el Desarrollo Económicos.

3.- Convenio 108 del Consejo de Europa: importancia del mismo. Principios rectores y definiciones básicas. El alcance normativo en España según la Sentencia 254/93, del Tribunal Constitucional.

Probablemente estemos ante el texto más influyente de todas las leyes y directivas sobre protección de datos actuales.

Características más destacables:

- Se prohíbe el tratamiento automatizado de informaciones referentes al origen racial, opiniones políticas, creencias religiosas u otras, salud sexual y condenas penitenciarias (artículo 6).
- Se hace hincapié en la seguridad de los registros de los datos (artículo 7).
- La exigencia de veracidad y correcta utilización de los datos (artículo 5). Mención del “Principio de Calidad de los Datos”.
- El reconocimiento del derecho por parte de los interesados a conocer la existencia de datos que les conciernen, la posibilidad de cancelarlos o corregirlos (Artículo 8).
- La facultad de recurrir ante cualquier trasgresión de los derechos antes mencionados (Artículo 8). En la actualidad, este artículo ha influido claramente en los dos procedimientos a los que puede recurrir cualquier ciudadano ante una vulneración de sus derechos: el principio de tutela de derechos y el procedimiento sancionador, hoy recogidos en nuestra Ley 15/99.
- Los límites que el Convenio establece al ejercicio del derecho a la libertad informática son (artículo 9.1):
 - La seguridad del Estado.
 - La protección de los demás derechos fundamentales.
- El artículo 3 del Convenio establece que su acción de protección comprende a "los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores públicos y privados"

Con este texto el Consejo de Europa, centrado en la defensa de los derechos humanos, se plantea oficializar la protección del derecho a la intimidad.²³ Y lo hace mencionando una serie de principios que ponen en todo caso límites al tratamiento automatizado de datos de carácter personal, como no podía ser de otra forma.

Se ha discutido si este Convenio era o no aplicable al ordenamiento jurídico español, de forma directa o a través de una Ley de Protección de Datos. El Convenio forma parte del ordenamiento jurídico español. Ahora bien, según señala el propio Convenio en su art. 4.1, "cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos", añadiendo este artículo en su párrafo 2 que "dichas medidas deberán adoptarse, a más tardar, en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte". Por tanto, la aplicación directa del Convenio dependerá del desarrollo legislativo posterior por el Estado. En cualquier caso, la trascendental sentencia 254/93 del Tribunal Constitucional, además de otros temas igualmente fundamentales, tratados en el punto correspondiente, se ocupa de la aplicabilidad o no aplicabilidad directa del Convenio 108. La respuesta es afirmativa. Textualmente, la Sentencia señala que "es lo cierto que los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 C.E., desde nuestra STC 38/1981". Ello a pesar de que el Tribunal Supremo confirmó que el Convenio de 1981, aunque se ha incorporado al ordenamiento jurídico español, precisa para su aplicación práctica el complemento de una actividad interna legislativa y reglamentaria que el Estado no ha desarrollado todavía, pero "el art. 8 del Convenio europeo, y muy especialmente su letra a), surte efecto directo: en él no se contiene un mero mandato a los Estados firmantes, sino el reconocimiento de un derecho, que puede ser invocado directamente por los ciudadanos, incluso en ausencia de regulación interna, porque no puede ser regulado de otra forma". Por último, "aun si se admitiera dialécticamente que el Convenio de 1981 no puede ser invocado directamente, constituiría una fuente de valor interpretativo de los derechos enunciados en el art. 18.1 de la Constitución, por imperativo de su art. 10.2; lo que llevaría a concluir que el contenido esencial de los derechos a la intimidad y a la propia imagen integra el derecho de los ciudadanos a conocer los datos que constan sobre ellos en los archivos automatizados de las Administraciones públicas".

²³ Loables intentos de leyes de protección de datos anteriores al convenio fueron la Ley de Hesse en Alemania (1970), la Datalag sueca (1973), la Privacy Act estadounidense (1974), la Constitución portuguesa (1976), la Ley de Protección de Datos francesa (1978) o la Data Protection Act inglesa (1984).

Por tanto, el reconocimiento de un derecho hace que el mismo pueda ser invocado por los interesados. Y en todo caso, este derecho tendría un valor importante para interpretar o incluso modular otros derechos reconocidos en nuestro ordenamiento jurídico. Desde este punto de vista, el Convenio si es aplicable, aún sin ley de protección de datos.

4.- La Ley 5/92, Reguladora del Tratamiento Automatizado de Datos (LORTAD).

Por fin, bastantes años después de que se promulgara la Constitución, hizo su aparición esta Ley. Tenemos por fin una legislación básica que regula los tratamientos automatizados de datos –en este caso, solo automatizados-, estableciendo unos límites a dicho tratamiento.

Resulta innegable que fue el Convenio 108 del Consejo de Europa el texto más influyente de esta norma, pero habrá que recurrir a la Ley Federal de 27 de enero de 1977 para la protección contra el abuso de datos sobre las personas con motivo del tratamiento electrónico de datos en la República Federal Alemana, para encontrar el texto donde la LORTAD se inspira. Si bien es cierto que la LORTAD acoge directamente principios como el de calidad de los datos o muchas definiciones del Convenio 108²⁴, existen muchas coincidencias desde luego nada casuales con la Ley Federal.

Se trata de la primera norma de derecho interno sobre la protección de datos personales. Como ya se ha mencionado anteriormente, nació en cumplimiento de la obligación de España de adoptar –antes de la ratificación del Acuerdo de Schengen- todas las iniciativas necesarias para completar el Ordenamiento interno español con el Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal.

Es necesario señalar, para situarla correctamente en el tiempo, que la LORTAD era un texto legal anterior en el tiempo a la Directiva 95/46/CE, pero en su elaboración se tuvo en cuenta una propuesta de Directiva²⁵ que sirvió de trabajo preparatorio de la propia Directiva

²⁴ Aunque para Juan José Martín Casallo López, no es óbice someter a una comparación a la LORTAD y al Convenio 108. Y ello porque el Convenio es un texto-marco que no se centra en ningún sector concreto y que recoge de manera quizás demasiado genérica ciertos principios y definiciones, mientras que la LORTAD es una ley que trata, en una treintena de artículos, resolver toda la problemática de la protección de datos directamente en un ordenamiento jurídico concreto. “*La Directiva 95/46/CE y su incidencia en el ordenamiento jurídico español*”. Madrid, 28, 29 y 30 de Octubre de 1996. Agencia de Protección de Datos.

²⁵ Propuesta de Directiva que la Comisión Europea presentada al Consejo el 18 de Julio de 1990. La misma fue modificada en el trámite parlamentario del Comité Económico y Social y el Parlamento Europeo. Ya se adelantaba el propósito de la Unión de aproximar las diferencias existentes entre las legislaciones de los países miembros al objeto de eliminar los obstáculos a la circulación de datos personales. La Propuesta de Directiva fue aprobada, y en el plazo de tres años, se debería incorporar a los

95/46/CE. El resultado es que recogía la mayor parte de los contenidos normativos y garantías legales no sólo del Convenio 108 del Consejo de Europa, sino también de la mentada norma comunitaria.

Dos son las partes principales en las que se divide la norma. Una general, alimentada por los preceptos delimitadores del ámbito de aplicación de la Ley, los principios reguladores²⁶ generales y, sobre todo, las garantías de la persona. Otra especial donde se concretan estos extremos, y donde se dividen a los ficheros en aquellos de titularidad pública o privada.

En la propia exposición de motivos²⁷, se mencionan conceptos como la privacidad y la intimidad, conceptos que no son en absoluto idénticos, ya que el de privacidad es más amplio que el de intimidad²⁸. Sin embargo, se alude en la mentada exposición que los elementos de la privacidad están principalmente definidos por el tiempo y el espacio. Desde luego, estos límites hoy en día han desaparecido: las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, las redes de telecomunicaciones apenas hace que éste tenga importancia, y la informática ha avanzado tanto que cada vez se requiere menos espacio para almacenar ingentes cantidades de información.

Sin duda, es muy descriptivo el siguiente párrafo de la exposición de motivos: "se hace preciso pues, delimitar una nueva frontera de la intimidad y del honor; una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, la proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ella referentes. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo, responde la presente Ley²⁹".

ordenamientos jurídicos internos de los países miembros. Como señala Emilio Del Peso Navarro, "en definitiva, en cierto modo, esta Propuesta de Directiva también la podemos considerar un antecedente inductor de la LORTAD." "*Ley de Protección de Datos, la Nueva Lortad*", Díaz de Santos, 2000. Pág. 11.

²⁶ Principios, por tanto, claramente inspirados en el Convenio 108 del Consejo de Europa.

²⁷ Exposición de motivos de la que carece la actualmente en vigor Ley 15/99, siendo éste uno de los aspectos más criticados de la misma.

²⁸ La propia exposición de motivos señala que "la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona". Respecto a la privacidad: "la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado"

²⁹ Para Miguel Vizcaíno Calderón, "La Ley de 1992 fue, en general, una buena Ley dictada en una situación de notable indiferencia social sobre las amenazas que las tecnologías de la información suponían para la privacidad de los ciudadanos". "*Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*", Civitas, 2001. Pág. 25.

5.- La Directiva 1995/46/CE, del Parlamento 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.

Es sin duda el “segundo gran hito en el desarrollo de un marco normativo para la protección de datos de carácter personal”.³⁰ Supuso, ante todo, la necesidad de una nueva consideración de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, a la luz de sus principios y de sus disposiciones.

Si la LORTAD hacía referencia nada mas que a los ficheros automatizados, cabría preguntarse que sucedía con los “ficheros físicos” o “ficheros en soporte papel”. La respuesta era clara: carecían de protección, ya que estaban excluidos. Sin embargo, si el bien jurídico protegido es la privacidad del individuo, ésta puede ser atacada igualmente desde un soporte u otro, indistintamente.

Carecía de sentido privar de igual protección a este tipo de ficheros. Ya en el año 1994, el profesor Ortí Vallejo aludía a que “los ficheros manuales presentan más amenazas para la vida privada y las libertades, pues cuando se componen de centenares de miles o incluso de millones de fichas, su puesta al día no es posible, con lo cual se mantendrían inexactitudes en los datos personales. Los ficheros automatizados frente a los manuales tienen la ventaja de poder ser destruidos fácilmente y ser susceptibles de medidas de seguridad más eficaces para hacerlos confidenciales...se puede concluir de lo expuesto, que existen razones de peso para atraer a la órbita de la LORTAD los ficheros manuales³¹”.

Como no podía ser de otra forma, el artículo 3.1 de la Directiva 95/46/CE establece que las disposiciones de la misma se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Ésta fue la principal razón de ser de la Directiva, y por supuesto, el motivo principal de modificación de la LORTAD.³²

³⁰ Rodrigo Bonadeo, “*Guía Práctica de Protección de Datos de Carácter Personal*”, Ediciones Experiencia, 2002

³¹ Antonio Ortí Vallejo, “*Derecho a la Intimidad e Informática*”, Comares, 1994.

³² El considerando 27 de la Directiva establece que: “Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un

Con esta Directiva³³, se establecía un sistema homogéneo a nivel comunitario en materia de protección de datos.

Las notas mas esenciales de este trascendental texto legal son las siguientes:

-Si bien es cierto que se repite la definición de “dato de carácter personal” como cualquier información que haga “identificada o identificable” a una persona, ahora esta definición se matiza. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

-La Directiva reconoce la imagen y el sonido como dato de carácter personal.

-Al igual que en la Ley, se establece el “Principio del Consentimiento Inequívoco del Interesado”: "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) El interesado ha dado su consentimiento de forma inequívoca".

-La Directiva considera especialmente protegidos los datos que hagan referencia a la ideología, a la religión, a las creencias, al origen racial, a la salud o vida sexual.

-El principal objetivo de la Directiva es "la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".

-Se recogen los derechos de acceso, modificación, cancelación y oposición. Verdaderos baluartes para que el individuo pueda controlar en todo momento la información que sobre su persona existe y es tratada. En suma, el vehículo vertebrador para ejercer su “habeas data”.

-Se recogen una serie de obligaciones de información para el responsable del fichero a la hora de recabar datos. Entre otras cosas, el mismo deberá de informar de quién es el

conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;”

³³ Posteriores Directivas que han abordado el tema pero desde el punto de vista de las comunicaciones electrónicas son la Directiva 97/66/CE, del Parlamento Europeo y del consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y la mucho más actual Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

responsable, la dirección a donde dirigirse el interesado para ejercitar su derecho de acceso, modificación, cancelación y oposición o de las posibles cesiones de los datos.³⁴

-Respecto a la seguridad de los datos, la Directiva establece que «dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse». En ese tiempo aún no se había redactado el Real Decreto 994/1999. El “Principio de Seguridad de los Datos” estaba igualmente recogido en la LORTAD.³⁵

6.- La Ley 15/99, de Protección de Datos de Carácter Personal. (LOPD).

La Ley Orgánica 15/99 ha traspuesto la Directiva 95/46/CE y, entre otras importantes novedades, ha extendido la protección a todo tipo de tratamientos, automatizados o no, en consonancia con lo estipulado en la Directiva, como no podía ser de otra forma.³⁶

Al proyecto se presentaron 114 enmiendas, y la Ponencia optó por proponer un nuevo texto completo.

La Ley tiene carácter de “orgánica”, pero no todos los preceptos tienen este carácter. Existe la conocida doctrina del Tribunal Constitucional por la que el mismo es proclive a reservar el rango de “orgánica” a aquellos preceptos que afronten directamente la regulación de los arts. 15 a 30 de la Constitución.³⁷

Según la Ley, el objeto es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas

³⁴ Recogido en el art. 5 de la Ley 15/99.

³⁵ Y ya se ha mencionado anteriormente que está recogido en nuestro art. 9. El Real Decreto se ha mantenido expresamente vigente. El no cumplimiento con este precepto, y por tanto, con el Real Decreto, supone una “falta grave” según el catálogo de sanciones recogido. Hoy, las empresas están asistiendo a un proceso de frenética actualización de estas medidas, ya que el plazo concluyó el pasado 26 de Junio de 2002.

³⁶ El Ordenamiento Jurídico Español estaba forzosamente obligado a adaptarse a la Directiva 95/46/CE. El art. 32 de la Directiva obligaba a los estados miembros a adoptar las disposiciones legales y administrativas necesarias para dar cumplimiento a lo establecido en aquella norma, a más tardar en un periodo de 3 años. En cualquier caso, la Exposición de Motivos se hace eco de que la LORTAD se ajustaba a la gran mayoría de las disposiciones de la Directiva. No obstante, era necesaria una reforma que diera como resultado la total trasposición de la Directiva.

³⁷ Establece la Disposición Final Segunda: “Los títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera, tienen el carácter de Ley Ordinaria.”

y especialmente de su honor e intimidad personal y familiar. En este sentido, es coincidente con lo dispuesto en la LORTAD.³⁸

Entre las características del texto, encontramos:

-El ámbito de aplicación de la Ley es francamente amplio. Así, “será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”. Si entendemos por dato “cualquier información concerniente a personas físicas identificadas o identificables” se deduce fácilmente que cualquier profesional, despacho, empresa, administración, organización, asociación (etc...) manejará datos de carácter personal susceptibles de entrar dentro del ámbito de la normativa.

-La creación de un nuevo derecho para los interesados, el “derecho de oposición”. Estos derechos, como se dice anteriormente, son los verdaderos “vehículos” con los que los interesados sustancian su derecho a la autodeterminación informativa.

-La modificación del régimen del Movimiento Internacional de Datos. Se suavizan los requisitos para proceder con ello.³⁹

-La limitación de las llamadas “fuentes accesibles al público”. Pasamos de una “cláusula abierta” en la Ley 5/92 a considerar fuentes accesibles al público únicamente las contenidas en la Ley.⁴⁰

-Tal y como se establece en la Directiva, se mantiene un régimen especial para aquellos datos considerados como “especialmente protegidos”. Así, se mantiene una necesidad de que exista un “consentimiento reforzado” para datos como los referentes a la salud o a la vida sexual, hasta el punto de que se especifica la forma en algunos casos en la que debe prestarse ese

³⁸ Para Pablo Lucas Murillo de la Cueva, el bien jurídico protegido es “la libertad informática”. *“Informática y protección de datos personales.”* Centro de Estudios Constitucionales. 1993

³⁹ Al respecto, la Instrucción 1/2000 de la Agencia de Protección de Datos, de 1 de Diciembre, dictada por el Director de la Agencia relativa a las normas por las que se rigen los movimientos internacionales de datos, es bastante clarificadora.

⁴⁰ Encontramos la siguiente definición en el art. 3 de la Ley al referirse a las fuentes accesibles al público: “Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación”

consentimiento –por escrito, en datos como la afiliación sindical⁴¹-, no olvidándose otros preceptos como los contenidos en la Constitución.⁴²

-Se establece la regla general de “no cesión” de datos de carácter personal. Pero, claro está, esta regla está sometida a una gran cantidad de excepciones. Los arts. 11 y 12 de la Ley establecen un complejo régimen de cesiones y comunicaciones de datos a terceros. Solo en los casos en los que estos dos artículos lo prevén, el Responsable del Fichero podrá ceder datos a terceros (empresa, profesional, administración, etc). Fuera de estos supuestos, estaremos ante una cesión ilícita de datos, sancionable por la Agencia de Protección de Datos. Además, la simple revelación de datos realizada por el responsable a persona distinta del interesado es considerada cesión, y requerirá del cumplimiento de una serie de condiciones especiales.

-Transferir datos de carácter personal a terceros países no siempre está permitido. Dada la heterogeneidad de ordenamientos, unos más protectores que otros, era necesario optar por un sistema garantista desde el punto de vista del interesado. Finalmente, la Ley ha transpuesto la norma del art. 12 del Convenio 108 del Consejo de Europa. Para no perjudicar el libre flujo de los datos, auténtica necesidad vital de empresas multinacionales –por citar solo un ejemplo-, se ha optado por permitir dicho flujo. Pero será necesario informar al Director de la Agencia de Protección de Datos de esta transferencia. Se puede aprovechar el momento de la creación del fichero para proceder a la información. Si no, será preciso modificar la inscripción del mismo en el Registro General de la Agencia de Protección de Datos, que es el órgano competente a estos efectos.

-En el art. 10 de la Ley encontramos una obligación genérica de “deber de secreto” impuesto al Responsable del Fichero y a quienes intervengan en cualquier fase del tratamiento de los datos. Encontramos una sujeción al secreto profesional respecto de los mismos, y al deber de guardarlos, matizando que estas obligaciones subsistirán aún después de finalizar sus relaciones con dicho Responsable.

⁴¹ Es necesario resaltar que estos datos considerados como “especialmente sensibles” gozan de un alto nivel de protección en el Real Decreto 994/1999. Así, en el art. 4.3 de su texto, encontramos que “los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.” Estas medidas son las necesarias para cumplir con el art. 9 de la Ley 15/99, Principio de Seguridad de los Datos. Entre ellos, existe la obligación para el responsable del fichero de proceder con el cifrado de los datos o un registro de accesos.

⁴² Art. 16.2 de la Constitución: “Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias”

-La Ley establece el régimen sancionador más alto de toda la Unión Europea. Este aspecto ha sido muy criticado por asociaciones, cámaras de comercio y empresas en general.

-Si bien es cierto que la ley se aplica a todo tipo de ficheros, llama la atención el plazo de moratoria que existe para los ficheros “preexistentes” a la entrada en vigor de la norma⁴³: 12 años. El legislador debe suponer, y con razón, las grandes modificaciones que el Responsable del Fichero deberá de implantar para adecuar a la normativa a los ficheros en soporte papel.

-Se adecuan algunas definiciones a lo dispuesto en la Directiva. El Responsable del Fichero pasa a denominarse –también- Responsable del Tratamiento.

-El encargado del tratamiento, como persona física o jurídica que presta un servicio al responsable del fichero, también puede ser sancionado⁴⁴. En supuestos de extralimitación de funciones del encargado del tratamiento, finalmente tendría responsabilidad.

7.- Interpretación del Tribunal Constitucional

Se aludía al principio de este estudio a la necesidad de que el Tribunal Constitucional se pronunciara en sentido positivo o negativo acerca de una serie de derechos que parece reconocer nuestra Carta Magna, pero que desde luego es necesario delimitar.⁴⁵

⁴³ La LOPD entró en vigor el 14 de Enero del 2000. La Disposición Adicional Primera establece que “los ficheros y tratamientos automatizados, inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente. En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.” Esto es aplicable para los ficheros preexistentes. Para los ficheros creados con posterioridad al 14 de Enero del 2000, la Ley es plenamente aplicable desde el principio.

⁴⁴ Dispone el art. 12.4 que “en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”

⁴⁵ Algunos autores hablan de “derechos no escritos”, sin duda “una nueva clase de derechos”. Manuel Jiménez de Parga y Cabrera señala que “los derechos no-escritos han de ser tutelados por la jurisprudencia, ya que las Constituciones proporcionan al intérprete un punto de apoyo, unas palabras (escasas a veces, lapidarias), sobre los que hay que efectuar, mediante una actividad creadora, la construcción del derecho fundamental”.Voto particular a la Sentencia 290/2000 del Tribunal Constitucional.

Se ha intentado analizar con profundidad la jurisprudencia del Tribunal Constitucional en esta materia, tratando de extraer las notas mas características al derecho a la libertad informática.

Sentencia 209/88: una aproximación al concepto de intimidad según el Tribunal Constitucional.

Dispone la Sentencia 254/93 que “la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades”. Parece necesario hacer una aproximación al concepto de “intimidad” para delimitar el de “libertad informática”⁴⁶.

La intimidad, en cuanto derivación de la dignidad de la persona, implica «la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana» (Sentencia 209/1988, fundamento jurídico 3.º) Además, el derecho a la intimidad no es absoluto, “como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho” (Sentencia 57/1994, fundamento jurídico 5.º).

La intimidad es la esfera personal de cada uno, en donde residen los valores humanos y personales, siendo un derecho fundamental para el desarrollo de la persona y de la familia además de ser un ámbito reservado a la curiosidad de los demás contra intromisiones e indiscreciones ajenas. La intimidad se ha protegido siempre de forma limitada. Por ejemplo, la violación de la intimidad domiciliaria, se centrará en aquellos casos en los que se produzcan registros no permitidos y vejaciones injustas ocasionados por los mismos. No solo se centrará dentro de este ámbito sino que además también afecta a otros campos como son las violaciones de la correspondencia y comunicaciones personales, intimidad laboral, obtención de datos relativos a la intimidad personal, familiar, o de terceros pertenecientes a la esfera de la familia. De tal forma que la intimidad es aquella esfera personal y privada que contienen comportamientos, acciones y expresiones que el sujeto desea que no lleguen al conocimiento público.

⁴⁶ Sobre todo cuando la misma sentencia concluye que la libertad informática forma parte del contenido esencial de los derechos fundamentales del artículo 18.1 CE. Y es que, esta libertad es también “además garantía de otros derechos, especialmente el honor y la intimidad”

Sentencia 53/1985: el Estado ha de tener una postura activa en la protección de los derechos fundamentales recogidos en la Constitución. Estos derechos recogen también facultades positivas para el individuo.

Se destaca esta Sentencia por la importancia que tiene de cara al legislador. Efectivamente: el Tribunal incide especialmente en la necesidad de que el Estado abandone su actitud pasiva respecto de algunos derechos fundamentales reconocidos en la Constitución. En suma, se hace eco del mandato constitucional del art. 18.4. El respeto a los derechos fundamentales no puede llevarse a cabo desde una postura “negativa” del Estado. Es necesario arbitrar normas que faculden a los interesados su ejercicio en una vía activa.

Resulta bastante ejemplificativo el siguiente párrafo:

“La doctrina ha puesto de manifiesto -en coherencia con los contenidos y estructuras de los ordenamientos positivos- que los derechos fundamentales no incluyen solamente derechos subjetivos de defensa de los individuos frente al Estado, y garantías institucionales, sino también deberes positivos por parte de éste”

Sentencia 254/93, 290/2000 y 292/2000: la doble vertiente de la libertad informática. Los límites de este nuevo derecho

La Sentencia 254/93 es la primera que establece la libertad informática como un derecho fundamental “en sí misma”. Es el “punto de apoyo” que se necesitaba para su articulación como tal. Lo que antes era una simple mención⁴⁷ constitucional es ahora un nuevo derecho con los límites perfectamente delimitados. Vamos a intentar delimitarlos.⁴⁸

Antes se aludía a la necesidad de que el Estado tenga una postura “activa” en la defensa de los derechos fundamentales. Pues bien, ello quedó perfectamente reflejado en el “caso Olaberry”, que se analiza a continuación.

El actor interpuso un recurso de amparo contra la administración por no facilitarle ésta una serie de informaciones referentes a su persona que se hallan en poder de la misma. A juicio del Tribunal Constitucional, la negativa por parte de la administración lesiona el derecho a la

⁴⁷ “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”. Artículo 18.4 de la Constitución Española.

⁴⁸ No se pretende restar importancia a lo estipulado en el mentado art. 18.4. Sin duda, la articulación de la Libertad Informática hubiera sido casi imposible sin este mandato constitucional.

“autodeterminación informativa” del individuo. El derecho estaba recogido, en ese año, en el Convenio 108 del Consejo de Europa⁴⁹. Ya se ha entrado a analizar la aplicabilidad del Convenio en el Ordenamiento Jurídico Español en el punto 3 de este estudio, por lo que al mismo me remito.

Dispone la Sentencia que “nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»”

Tenemos por tanto un doble carácter del derecho a la “autodeterminación informativa” o a la “libertad informática”. Por un lado, es una garantía de otros derechos, los recogidos en el art. 18. Por otro lado es “un derecho en sí mismo”, cuyo objetivo final es “frenar el tratamiento ilegítimo de datos”, o al menos “poner límites al mismo”.

Obviamente, el reconocimiento de este derecho hace que se necesiten fórmulas para que los ciudadanos lo puedan ejercer. Y desde luego, no es posible “la negativa por respuesta” de la administración. En todo caso, los responsables estarían obligados a facilitar la información a los interesados cuando éstos lo requieran:

“La «libertad informática», reconocida por el art. 18.4 de la Constitución, ya no es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de habeas data.⁵⁰”

Es cierto que una Ley de Protección de Datos y la existencia de la Agencia de Protección de datos aclararía muchas cosas, pero ello no es óbice para que se reconozcan ciertos derechos, sobre todo cuando existen mención de los mismos –aunque indirectamente- en la Constitución Española y cuando han sido señalados en los Convenios Internacionales:

⁴⁹ Mas concretamente, en el artículo 8, letras a) y b) del mismo

⁵⁰ Antecedente 5

“La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada. Pero ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto imprescindibles para proteger el derecho fundamental a la intimidad en relación con los ficheros automatizados que dependen de los poderes públicos. Ni tampoco exonera a las autoridades administrativas del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan datos personales de éstos, ni del deber de satisfacer las peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades.⁵¹”

Por su parte, la Sentencia 290/2000, de 30 de noviembre, es consecuencia de una serie de recursos (201/1993, 226/1993 y 236/1993) interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y 56 Diputados contra determinados artículos de la Ley 5/1992. La Sentencia solo lo estudiaremos en cuanto configuradora de este derecho, obviando la controversia con el Parlamento de Cataluña, por no ser objeto del trabajo.

Los Magistrados Manuel Jiménez de Parga y Cabrera y Rafael de Mendizábal Allende firmaron sendos votos particulares. Los mismos atribuyen a la dignidad de la persona humana y a los derechos inviolables que le son inherentes en cuanto fundamento del orden político y de la paz social una posición prevalente porque constituyen principios constitucionalizados a partir de los cuales nacen todas las normas legitimadas por la Constitución.

Se destaca los siguientes párrafos de esta trascendental Sentencia:

“El derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado...el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 de la CE otorga, sino los datos de carácter personal.”“...pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros...dicha peculiaridad radica en su contenido, ya

⁵¹ Fundamente Jurídico 9

que... el derecho a la protección de datos atribuye un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva el poder de disposición sobre los datos personales.”

El tribunal reconoce el derecho de libertad informática como un derecho inherente a la persona, objeto de protección.

Respecto a la Sentencia 292/2000, en este caso se planteó por un Recurso de Inconstitucionalidad realizado por el Defensor del Pueblo, respecto de los artículos 21.1 y 24.1 y 2 de la Ley 15/1999. Una vez, decir que no es objeto del trabajo el estudio de los preceptos finalmente declarados inconstitucionales. Pero si es interesante decir que en la Sentencia se establecieron límites al derecho de información del art. 5.1 respecto de las administraciones públicas: en este caso, solo la defensa nacional, la seguridad pública o la persecución de una infracción penal. También, decir que las administraciones sólo podrán –ahora- denegar los derechos de acceso, rectificación y cancelación ejercidos legítimamente por los interesados cuando estemos dentro de los supuestos del art. 23 de la Ley.⁵²

Si que es interesante decir que nuevamente el Tribunal Constitucional, por medio de la Sentencia que analizamos, viene a establecer el derecho a la protección de datos como derecho fundamental autónomo, cuyo contenido está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999. En virtud de este derecho fundamental, el ciudadano, con carácter general, “puede decidir sobre sus propios datos”.

⁵² Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Destacar nuevamente que el objeto de protección no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal. Ello sin perjuicio del establecimiento de un régimen especial para un cierto tipo de datos.

Sentencia 143/94: el principio de finalidad en la recogida de los datos.

Se alude a esta sentencia por la importancia que tiene en relación con el principio de finalidad de los datos de carácter personal. Como ya se ha mencionado, este Principio está recogido en nuestra Ley 15/99: “los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”.

No se pretende entrar a estudiar la posible vulneración del art. 24.1 de la Constitución Española, ya que no es el objeto del presente trabajo. Se plantea, principalmente, la vulneración de una serie de derechos fundamentales imputable directamente a la normativa reguladora del Número de Identificación Fiscal (Real Decreto 338/1990, de 9 de marzo, y Orden Ministerial de 14 de marzo de 1990, de desarrollo del anterior).

En este caso, el Tribunal Constitucional concluye que la finalidad es totalmente legítima, y que la recogida de datos no es desproporcionada en ningún caso en base a las siguientes razones:

-El Real Decreto impugnado presenta una “clara orientación tributaria”. El objeto del mismo es establecer “fórmulas de lucha contra la defraudación fiscal mediante instrumentos de seguimiento y control de las actividades que, estando previstas como gravables, se realicen por los sujetos obligados al pago de los tributos”. Por tanto, finalidad justificada.

-La recogida de datos planteada en el Real Decreto en absoluto es desproporcionada: “tampoco puede considerarse la norma como desproporcionada o contraria al contenido general del derecho, habida cuenta de la estricta relación de causa a efecto existente entre el contenido de la información y la finalidad descrita; del carácter restrictivo y teleológicamente orientado a operaciones sujetas a tributación con que se concibe la carga de informar del N.I.F. Como instrumento de control y, sobre todo, de la adecuación de los destinatarios de la información (la Administración) desde la perspectiva de la finalidad perseguida por la norma (STC 240/1992, fundamento jurídico 7.)”. Por tanto, no existe desproporción.

Si no existe desproporción en la recogida y la finalidad está en todo caso justificada, se respeta el principio de finalidad.⁵³

Sentencia 11/98 y 60/98: utilización de datos para finalidades no permitidas.

Se vuelve a estudiar el trascendental concepto de finalidad de los datos, aunque los supuestos son distintos. En estas sentencias se trata la problemática de utilización de datos especialmente protegidos para finalidades distintas. Concretamente datos de afiliación sindical.⁵⁴

Los datos deben de destinarse en todo caso en consonancia con la finalidad para la que fueron recabados. Si existen supuestos de incompatibilidades en este sentido, y además los datos son considerados como “especialmente protegidos”, el bien jurídico protegido se lesiona en un grado superior. Ello demanda mayores responsabilidades para el Responsable del Fichero:

“Un dato que pertenece a la privacidad del trabajador, que posee la Empresa con una exclusiva finalidad -descontar la cuota de afiliación sindical- sirve para impartir instrucciones al sistema informático y que se descuenten todos los días de paro a los que tienen la clave 893, correspondiente a los afiliados a CC.OO. Resulta ilustrativo que por estos mismos hechos la Agencia de Protección de Datos en Resolución de 18 de diciembre de 1995, haya impuesto a RENFE una multa de 50.000.001 pesetas por una infracción tipificada como muy grave en el art. 43.4 c) de la Ley Orgánica 5/1992.” (Sentencia 11/98)

No hay dudas de que un dato de afiliación sindical, en un contexto distinto al que fue recabado, puede dañar la intimidad del individuo:

“Es de señalar que la STC 292/1993 ha abarcado en el arco protector de tal Ley el dato de la afiliación sindical como atinente a la ideología del individuo. La utilización desviada de un dato cedido voluntariamente para otro fin puede incidir directamente en la intimidad del individuo” (Sentencia 11/98).

Otra nota interesante referente a la finalidad de los datos:

⁵³ Esta Sentencia parece estar claramente inspirada en la dictada por el Tribunal Constitucional Alemán, estudiada anteriormente. En la misma se hace mención a que en los supuestos de recogida de datos debe prevalecer un interés general, y existir un mandato constitucional.

⁵⁴ Se recuerda que en un punto anterior se advertía sobre la posible vulneración del principio de finalidad de los datos, ya que en muchísimas ocasiones los datos se utilizan para finalidades distintas.

“Partiendo de estas premisas, en este caso debe tenerse en consideración que la afiliación del trabajador recurrente a determinado Sindicato, se facilitó con la única y exclusiva finalidad lícita de que la Empresa descontara de la retribución la cuota sindical y la transfiriera al Sindicato, de acuerdo con lo establecido en el art. 11.2 L.O.L.S⁵⁵. Sin embargo, el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al período de huelga.” (Sentencia 11/98)

Además, la vulneración del principio de finalidad no está sujeto a dolo ni a culpa, se trata de una responsabilidad “objetiva”, al igual que ocurre cuando se lesiona otro derecho fundamental:

“En este caso la vulneración de derechos fundamentales no queda supeditada a la concurrencia de dolo o culpa en la conducta del sujeto activo, a la indagación de factores psicológicos y subjetivos de arduo control. Este elemento intencional es irrelevante y basta constatar la presencia de un nexo de causalidad adecuado entre el comportamiento antijurídico y el resultado lesivo prohibido por la norma.” (Sentencia 11/98).

La Sentencia 60/98 reproduce a la 11/98 en la mayoría de los términos, al igual que la 94/98.

Sentencia 202/99: necesidad del consentimiento expreso para tratar datos especialmente protegidos.

Se plantea en este supuesto muchos y muy variados aspectos, tales como:

-El problema del consentimiento. La necesidad del consentimiento expreso para los datos especialmente protegidos.

-El régimen de los datos especialmente protegidos.

-Las excepciones para recabar datos sin necesidad del consentimiento.

-En general, la posible vulneración del principio de calidad de los datos.

⁵⁵ Ley Orgánica de la Libertad Sindical. La sentencia declara que se lesiona el art. 28 –Libertad Sindical- de la Constitución en relación con el 18.4 –Libertad Informática-.

Todo ello en un marco donde el objeto son los datos de bajas laborales, especialmente protegidos por tanto.

El que una entidad crediticia tenga una base de datos denominada “absentismo con baja médica” sin el conocimiento de sus empleados y por tanto sin el consentimiento de los mismos, atenta con el “Derecho a la Libertad Informática” de ellos, máxime cuando a esta información pueden acceder no solo facultativos, sino también personal que no tiene la consideración de profesional sanitario:

“Según se ha consignado en los antecedentes, el ahora solicitante de amparo denuncia que la existencia en la entidad crediticia «Banco Hispanoamericano, S.A.», en la que presta sus servicios, de una base de datos denominada de «absentismo con baja médica» en la que figuran los diagnósticos de las enfermedades que dieron origen a una situación de baja laboral por incapacidad temporal, sin consentimiento expreso de los afectados y sin que la entidad haya alegado en ningún momento un interés contractual suficiente, vulnera los derechos fundamentales proclamados en el art. 18 C.E., en especial en su apartado cuarto. Denuncia que se extiende a la negativa a la cancelación de los datos obrantes en el fichero, así como al hecho de que puedan tener acceso a la base, tanto los cuatro médicos de la empresa como un empleado de ésta, adscrito al área de personal, que no goza de la condición de facultativo y que es quien proporciona la clave de entrada en el sistema, con lo que no quedaría garantizada la confidencialidad de los datos. Finalmente, pone de manifiesto que la base de datos en cuestión no está dada de alta en la Agencia de Protección de Datos, no existiendo, por tanto, un responsable oficial del fichero”

El Tribunal concluye que:

“A la vista del contenido del fichero, forzoso resulta convenir que su mantenimiento no se dirige a la preservación de la salud de los trabajadores, sino al control del absentismo laboral, lo que, por otra parte, resulta plenamente acorde con la denominación «absentismo con baja médica» que recibe el fichero. Consecuentemente, la creación y actualización del fichero, en los términos en que se ha llevado a efecto, no puede ampararse, frente a lo sostenido por la empresa, en la existencia de un interés general (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica -y consentida por los afectados- del estado de salud de los trabajadores en función de los riesgos

inherentes a su actividad laboral, sino tan sólo la relación de períodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador.”

Es necesario el consentimiento expreso para tratar datos especialmente protegidos, fuera de los casos excepcionados en la LORTAD. En este caso, la Ley de Prevención de Riesgos Laborales y la Ley General de la Sanidad desde luego no autoriza al Responsable del Fichero a recabar la información que se estaba manteniendo, sobre todo cuando la finalidad parece no ir en consonancia con lo dispuesto en esas dos Leyes. La finalidad parece ser el control del absentismo laboral, y ello no está entre las excepciones anteriormente mencionadas:

“Consiguientemente, debemos concluir que el tratamiento y conservación del diagnóstico médico en la mencionada base de datos sin mediar consentimiento expreso del afectado incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 C.E.”

8.- Conclusión

Se ha tratado en este estudio de, por una parte, ver la evolución de este “novísimo derecho fundamental”⁵⁶ desde la década de los 60-70 hasta la actualidad, y por otra, de examinar las notas más fundamentales que sobre el mismo ha argumentado nuestro Tribunal Constitucional.

Llama la atención que desde un primer momento, los legisladores hayan tenido claro que la informática puede llegar a ser un peligro para la persona. Esto, que hoy en día puede parecer evidente, no lo era en absoluto hace tres décadas. El esfuerzo previsor es patente, y ya no sólo respecto a nuestros constituyentes: textos como el de la OCDE o la Resolución 509 de 1968 hablan por sí mismos.

La “libertad informática” es un derecho autónomo, pero en todo caso muy unido a los contenidos en el art. 18.1 de la Constitución Española. Ante todo, es el derecho que tienen todas las personas a controlar el flujo de informaciones existentes sobre las mismas.

Los Convenios Internacionales pueden ser plenamente efectivos en cuanto configuradores de derechos fundamentales reconocidos en la Constitución. En este sentido, el “caso Olaberry” demostró que es necesaria una postura “pro-activa” de la administración a

⁵⁶ Rafael de Mendizábal y Allende

facilitar la información que se le requiera sobre los administrados. Ya no se configura este derecho desde la parcela negativa o “preventiva”.

Todos los datos están sometidos al principio de la finalidad, pero es cierto que el no sometimiento a este principio de datos considerados como “especialmente protegidos” hace que se produzca una lesión mayor. Piénsese si se utilizaran datos de salud de los individuos para la venta de productos ortopédicos.

En la actualidad, la “libertad informática” se encuentra perfectamente delimitada por nuestro Tribunal Constitucional, a la vez que existe un cada vez mayor interés en la sociedad por cuidar y tratar, legal y lealmente, la información de carácter personal. Sin duda, el carácter de “autónomo” de este derecho ha hecho que se le de la importancia necesaria.

Alumno: Alfonso Villahermosa Iglesias

Asignatura: “Jurisprudencia sobre protección de datos”.

BIBLIOGRAFÍA

-CASTAÑEDA, Alberto, BONADEO, Rodrigo y SANCHEZ, Jesús, “*Guía Práctica de Protección de Datos de Carácter Personal*”, ed. Ediciones Experiencia, Barcelona, 2002.

-DAVARA RODRIGUEZ, Miguel Angel. “*Factbook de comercio electrónico*”. Aranzadi, Madrid, 2002.

-DEL PESO NAVARRO, Emilio, “*Ley de Protección de Datos, la Nueva Lortad*”, ed. Díaz de Santos, Madrid, 2000.

-ECIJA ABOGADOS, “*Factbook de protección de datos*”, Aranzadi, 2003.

-EXTXEBERRI GURIDI, José Francisco, “*La protección de datos personales en el ámbito de la investigación penal*”. Agencia de Protección de Datos. Agencia de Protección de Datos. 2001.

-FERNANDEZ DOMINGUEZ, Juan José, y RODRIGUEZ ESCANCIANO, Susana “*Utilización y control de datos laborales automatizados*”. Agencia de Protección de Datos, 2001

-“*Manual Protección de Datos para las Administraciones Públicas*”. Agencia de Protección de Datos de la Comunidad de Madrid. Civitas. 2004.

-MARTIN CASALLO LÓPEZ, Juan José, “La Directiva 95/46/CE y su incidencia en el ordenamiento jurídico español”. Madrid, 28, 29 y 30 de Octubre de 1996. Agencia de Protección de Datos.

-MARZO, Ana, MARZO, Iciar. “*Internet. Claves legales para la empresa*”. Civitas, Madrid, 2002.

-Memoria de la Agencia de Protección de Datos (1995-2002)

-Memoria de la Agencia de Protección de Datos de la Comunidad de Madrid de 2002.

-RUIZ MIGUEL, Carlos, “El Derecho a la Intimidad Informática en el Ordenamiento Jurídico Español”. Universidad de Santiago de Compostela.

-Sentencias 53/1985, 254/93, 143/94, 11/98, 60/98, 94/98, 202/99 y auto 642/1986 del Tribunal Constitucional.

-VIZCAINO CALDERON, Miguel, “*Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*”, ed. Civitas, Madrid, 2001.