Algunas cuestiones jurídicas relativas a la documentación automatizada: confidencialidad y protección de los datos

Carlos Manuel DA COSTA CARBALLO
Profesor Titular EUBD Complutense

INTRODUCCION

Se han detenido a pensar alguna vez en cuántos bancos de datos puede estar nuestra información personal y en el uso que de la misma pueden estar haciendo otras personas sin que nosotros tengamos notificación alguna de este hecho.

Si en este momento repasamos mentalmente en cuantos bancos de datos automatizados podemos estar incluidos, nos encontraremos con un buen número de ellos. Veamos. Desde el mismo momento en que venimos a la vida, nuestros padres se encargan de inscribirnos en el Registro Civil, siendo este el primer banco de datos en el que quedamos «almacenados», si se me permite la expresión. A continuación, si somos bautizados, pasamos a un segundo banco de datos que es el de la propia Iglesia. Pasarán probablemente unos años hasta que volvamos a entrar en un banco de datos, siendo este el del Ministerio de Educación y Ciencia en cuanto empezamos a ir a la escuela. Si seguimos estudiando y entramos en la Universidad pasaremos al cuarto banco de datos que no es otro que el del Centro de Cálculo de la Universidad en la que cursemos nuestros estudios. Si acabamos la carrera y empezamos a ejercer nuestra profesión, con toda probabilidad tendremos que entrar a formar parte de algún Colegio Profesional, además de que si conseguimos entrar en el mercado laboral, tanto si es por cuenta ajena como si es en una empresa, estaremos desde ese preciso momento registrados en un nuevo banco de datos que es el de la propia empresa. A esto debemos sumar otros dos bancos de datos que serán el de la Seguridad Social y el conocido por el nombre de *Berta* del Ministerio de Economía y Hacienda.

Revista General de Información y Documentación, Vol. 2 (2), 17-49, Edit. Complutense, Madrid, 1992

No se acaba aquí nuestra andadura por los bancos de datos automatizados puesto que si en algún momento de nuestra vida tenemos que ingresar en un Centro Sanitario por el motivo que sea, quedaremos registrados por partida doble. En el momento de entrar, en el Servicio de Admisión de enfermos. Cuando nos den el alta, en el Archivo Central de Historia Clínicas, sin contar que podemos pertenecer a algún Seguro Médico Privado, a alguna Sociedad Científica relacionada con nuestra profesión, a alguna Organización Política, además de los bancos de datos siguientes: Cuerpos de Seguridad del Estado (DNI, Pasaporte, etc., es decir en el famoso ordenador *Rita* del Ministerio del Interior), Ministerio de Defensa (cuando hicimos el Servicio Militar), algún Banco (por la cuenta corriente o cartilla de ahorros), Cámara de la propiedad (por nuestra vivienda), Compañía Telefónica, Compañía del Gas, Compañía de la Luz, Compañía del Agua, Compañía de Seguros, etcétera[1].

Es decir, oficialmente nuestros datos personales se encuentran repartidos por un gran número de bancos de datos automatizados, pero oficiosamente todos sabemos que estamos en muchos más pues ¿quién no recibe una buena dosis de propaganda de lo más variado en forma de revistas especializadas o generales, folletos de tal o cual diccionario enciclopédico, sin que en la mayoría de las ocasiones nosotros hayamos dado nuestros datos a nadie relacionado con esa propaganda? Cabe preguntarse por lo tanto:

— ¿quién está autorizado a reunir y almacenar nuestra información?,
— como ciudadanos de un estado libre y democrático, ¿tenemos derecho a saber qué tipo de información hay en las diferentes computadoras en las que se encuentran nuestros datos?,
— quién está autorizado a recibir información acerca de cada uno de nosotros y qué uso se va a hacer de ella?,
— si se producen errores en la entrada de nuestros datos que pueden dar lugar a daños morales de nuestra persona, ¿quién es el responsable, el que introdujo los datos, el que recibe la información y la utiliza inadecuadamente, el dueño de la computadora o el que proporciona la información?,
— ¿quién o quiénes están autorizados a proporcionar nuestros datos?,
— ¿está suficientemente protegida la intimidad de nuestra información en un banco de datos automatizado?,

---

[1] Para hacerse una idea de los bancos de datos en los cuales puede estar nuestra información, se pueden consultar los siguientes catálogos:

FUINCA: *Catálogo de servicios de información electrónica españoles*. Fuinca, 5.ª ed., Madrid, 1988, 284.

PEINADO BENAYAS, M.ª del Carmen: *Aplicaciones sociales de las nuevas tecnologías de la información en España*. Fundesco (Colección Informes), Madrid, 1989, 526.

— ¿se puede regular de alguna forma el acceso a nuestra información por parte de terceras personas?

Esto es solamente un ejemplo de cuestiones que podemos hacernos en un momento determinado, pero no cabe duda de que el lector se estará haciendo otro tipo de preguntas con respecto a este mismo tema, de la misma forma que otros pueden estar pensando que para determinadas investigaciones se necesitan datos estadísticos fiables que sólo pueden obtenerse si contamos con unos buenos bancos de datos. Por lo tanto vemos que ya hay un conflicto entre dos derechos constitucionales: el derecho a la información y el derecho a la protección de los datos, es decir, de un lado nos encontramos con que hay que preservar la confidencialidad de las personas y regular de alguna forma la protección de los datos, y de otra parte vemos la necesidad de que las leyes y reglamentos no obstaculicen innecesariamente los estudios que puedan hacerse con nuestros datos.

Vistas así las cosas habría que buscar el equilibrio entre la protección de los datos y la recopilación de información sobre las personas, para que no sucedan casos como los acaecidos hace poco tiempo en Estados Unidos, donde la compañía de software Lotus Development pretendía desarrollar un producto en CD-ROM (que se llamaría MarketPlace Households) donde se recogerían los hábitos de compra de las amas de casa americanas y donde aparecían los nombres, edades, direcciones, estado civil y otra serie de datos personales de unos 120 millones de ciudadanos. Los datos se elaboraron a partir del Censo de los Estados Unidos y datos fiables de consumidores reunidos por la compañía Equifax Inc., una de las agencias de encuestas más importante del país. Los datos fueron recogidos sin pedir permiso a los interesados ni se notificó su inclusión en tal proyecto. Más de 30.000 personas llamaron a la compañía diciendo que Marketplace Households «*...represented an abuse of private information*» o «*...its action was an invasion of privacy*»[2]. El proyecto fue abandonado en febrero.

---

[2] Este caso ha hecho revivir los viejos debates acerca de las libertades civiles. Puede seguirse el suceso y otros similares (Philip Morris y su promoción de la Declaración de Derechos por teléfono; Wats Marketing de Omaha y su sistema de telecompra llamado Donnelly Marketing's Fast Data System; Worldata y su base de datos de las personas que ganaban más de 30.000 $ para promocionar vacaciones bajo el nombre de Holiday Inn Great Rates List, etc.) en los siguientes artículos:

ECONOMIST (The): «Computers and Privacy. The Eye of the Beholder». *The Economist*, May 4th, 1991, 21-23.

LEWIS, Peter H.: «The Executive Computer. Why the Privacy Issue Will Never Go Away?». *The New York Times*, April 7, Sunday, 1991, 4.

ROTENBERG, Marc: «In Support of a Data Protection Board in the United States». *Goverment Information Quarterly*, 1991, vol. 8, n.° 1, 79-93.

Un segundo ejemplo que nos sobresaltó a los españoles fue la desarticulación de una red de traficantes de datos por efectivos de los cuerpos de seguridad del Estado[3]. Si recuerdan, esta red había llegado a elaborar un registro con 47 datos diferentes (sensibles y no sensibles) sobre 21 millones de españoles, comprando la información a personas de algunos Ministerios, empresas privadas, bancos, etcétera, para revenderlos después a determinadas empresas financieras y de servicios que los utilizarían para conocer aspectos muy concretos de 21 millones de potenciales clientes. La operación que acabó con esta red de delincuentes llevaba en marcha varios meses desde que un ciudadano español interpuso una denuncia en la que alegaba haber recibido publicidad en su domicilio donde constaba su segundo nombre, aspecto éste que puede parecer de escasa importancia salvo por el pequeño detalle de que nadie lo conocía (a excepción de su familia y la Seguridad Social), demostrándonos una vez más el vacío legal que hay en torno al uso descontrolado que se está produciendo de las nuevas tecnologías informáticas.

Acciones similares se producen en el mundo con el permiso de los interesados[4].

---

[3] Este suceso puede seguirse en los siguientes artículos:

— PAIS (EL): «La policía investiga a los funcionarios que vendían datos privados a una red de traficantes». *El País*, Año XVII, n.º 5.374, sábado 11 de enero, 1992, p. 16.

— «Los piratas informáticos obtenían datos de dos bancos y seis cajas». *El País*; Año XVII, n.º 5.375, domingo 12 de enero, 1992, p. 22.

— «Los traficantes de datos informáticos incluían información íntima en su oferta, según la policía». *El País*, Año XVII, n.º 5.376, lunes 13 de enero, 1992, p. 20.

— DIARIO 16: «Ingresa en prisión el <<cerebro>> de la banda informática». *Diario 16*, lunes 13 de enero, 1992, p. 11.

— PAIS (EL): «Detenidos un funcionario de Trabajo y otros dos empresarios de la red de "piratas" informáticos». *El País*, Año XVII n.º 5.377, martes 14 de enero, 1992, Editorial y p. 20.

— DIARIO 16: «Cuatro funcionarios de Industria y Trabajo vendieron información confidencial a los traficantes de datos». *Diario 16*, martes 14 de enero, 1992, p. 15.

— PAIS (EL): «El cerebro de la red del fraude informático sale de Carabanchel disfrazado». *El País*, Año XVII n.º 5.378; miércoles 15 de enero, 1992, p. 20.

Fue éste un típico delito de cohecho por parte de los funcionarios que vendían datos privados, delito que consiste en aceptar cualquier presente por realizar un acto injusto relativo a sus funciones que constituya un delito, aunque este acto no esté prohibido legalmente [DIAZ-MAROTO y VILLAREJO, Julio, y SUAREZ GONZALEZ, Carlos J.: *Código Penal y Legislación Complementaria*. Civitas (Biblioteca de Legislación), Madrid, Libro II (Delitos y sus penas), Título VII (De los delitos de los funcionarios públicos en el ejercicio de sus cargos), Cap. IX (Del cohecho), 1991, arts. 385 a 393, 200-202].

[4] Veamos otros dos ejemplos: *Business List-on-Disk* es una base de datos para ordenadores IBM compatibles que cuesta 750 $ por año de licencia creada por Trinet America, Inc. y la American Business Information, Inc. de Omaha, que contiene información de 9,2 millones de

Podríamos preguntarnos, llegados a este punto ¿por qué se producen estos sucesos? La causa última de esta situación ha sido el rápido progreso de la tecnología documental, que va mucho más diligente y siempre por delante que el desarrollo del propio derecho legislativo, y el modo de resolverlo sería establecer unas normativas nacionales e internacionales para el uso y protección de los datos personales por parte de las instituciones públicas o privadas, o en su defecto por cualquier persona que tenga acceso a nuestros datos.

Por lo tanto, el objetivo que perseguimos en esta Lección Magistral es desarrollar una investigación lo mas detallada posible a través de la legislación vigente del problema de la protección de los datos personales informatizados, realizando para ello un estudio comparativo entre dos foros importantes, Estados Unidos de América y la Comunidad Económica Europea, con respecto a nuestro país y ver, en que medida nuestras ordenanzas actuales son equiparables a las de las demás naciones e incluso pronunciarnos, si es posible, acerca de si nuestras leyes son mejores, iguales o peores que las de estos territorios.

Para conseguir este objetivo el desarrollo del tema será el siguiente:

I. El problema de la Confidencialidad de la información en los bancos de datos automatizados.
II. Protección de los datos.
III. Niveles de control legislativos.
   III.a) Primer nivel: códigos de ética profesionales, tradiciones escritas, juramentos y compromisos.
   III.b) Segundo nivel: legislación positiva.
   III.c) Tercer nivel: directivas, recomendaciones y reglamentos.
IV. El respeto a la intimidad de las personas: análisis de la legislación actual:
   IV.a) Legislación informática en los Estados Unidos de América.

---

empresas públicas y privadas del suroeste americano donde se incluye el nombre, la dirección, número de empleados y una descripción de cada una de las empresas (capital, propiedades, números de teléfono, contactos, etc.).

En nuestro país también hay casos similares. La Comisión Interministerial de Ciencia y Tecnología recogió datos del personal investigador que gozaba de alguna beca o ayuda I+D o de cualquier otro tipo. Después mandaba diskettes a todos los investigadores para que adjuntaran en dos ficheros distintos una serie de datos personales y académicos para actualizar sus bases de datos y para incluirlos en «*...las bases de datos europeas e internacionales relativas a personal, empresas y organismos interesados en I+D; intercambio de información;...*».

En ambos casos hay conformidad de los interesados, pues si no te interesa mandar tus datos no los mandas, pero las cuestiones son las de siempre, ¿qué se hace con esos datos?, ¿quién los gestiona?, ¿quién los utiliza y para qué?, etcétera.

I. EL PROBLEMA DE LA CONFIDENCIALIDAD DE LA INFORMACION EN LOS BANCOS DE DATOS AUTOMATIZADOS

La informática como herramienta ha servido para agilizar las tareas que en tiempos no muy remotos llegaban a ocupar a varias personas y durante varias jornadas de trabajo, pero al tener como material de trabajo los datos, es decir la información que se genera en el quehacer cotidiano de las personas, su uso implica riesgos que pueden atentar contra la intimidad de los individuos.

Por esto habría que diferenciar entre los bancos de datos que contienen información que podríamos llamar del dominio público, de aquellos otros cuya información puede constituir materia reservada. En el primer tipo de bancos de datos habría que tomar las medidas de seguridad típicas de cualquiera de estos productos, mientras que en el segundo habría que tomar una serie de medidas especiales para proteger la información que contienen.

Por lo tanto por medio del fraude, el mal uso de la informática, el «pirateo» de datos o programas, el sabotaje y cualquier acción punitiva que ocasione una agresión lesiva de la información contenida en un banco de datos se atenta contra la intimidad de las personas. En este momento vamos a ocuparnos de los problemas éticos y legislativos del uso de la información.

Partiendo de que cualquiera de nosotros vamos a trabajar con bancos de datos informatizados en los que hay o puede haber información reservada, la primera duda que se nos plantea es si la intimidad de las personas está a salvo en estas máquinas, y por lo tanto si se pueden poner en peligro algunos derechos fundamentales de las personas.

Para intentar analizar estos aspectos concretos, tendremos necesariamente que empezar definiendo ¿qué es la intimidad o privacidad de las personas?

La intimidad o privacidad de las personas puede definirse como «...la libertad, en el entorno inmediato del individuo, frente *a la intromisión no deseada de otras personas*»[5], es decir, se trata de aquella parte interior del ser humano

[5] SANCHEZ GONZALEZ, Miguel: «Problemas éticos y legislativos (I)». *El Médico, profesión y humanidades*, septiembre, Madrid, 1990, 49-50.

que es reservada, y que por lo tanto tiene que ver con la vida privada de cada uno. En la misma línea podemos decir que se encuentra la siguiente definición de intimidad: «*La intimidad es un tipo de independencia especial que puede entenderse como un esfuerzo para asegurar la autonomía (...) si resulta necesario frente a las presiones de la sociedad moderna*»[6].

Pero a lo largo de la historia esto no fue así ni mucho menos. En la Edad Media, por ejemplo, no había una separación clara entre la vida pública y la vida privada, y la mayoría de las acciones o actos que se pueden entender que pertenecen a la vida privada se realizaban en público.

Es precisamente en nuestra sociedad actual cuando al pretender elegir libremente nuestra forma de vida cada uno de nosotros hemos creado la *vida privada* condicionada, de una parte por los valores y actitudes que se adoptan en nuestro entorno, y de otra por el desarrollo tecnológico de la sociedad en la que estamos inmersos. Jurídicamente no toma forma hasta que Louis D. Brandeis y Samuel D. Warren «inventan» el derecho a la vida privada[7].

Por lo tanto, si la intimidad es esa parte de las personas que consideramos reservada, qué entendemos por confidencialidad. Siguiendo al mismo autor, la confidencialidad sería el conjunto de «*... todas las informaciones que, por una u otra razón, no deben hacerse públicas*»[8].

Pero este *derecho a la vida privada* tardó en ser asumido por todos, ya que algunos admitían, por ejemplo que «*...en cierto punto, el interés del público por obtener información adquiere predominio sobre el deseo de vida privada del individuo*»[9]. Si a esto sumamos la intrusión de las computadoras en la vida

---

[6] La definición es de Clinton Rossiter citado por SARTORI, Giovanni: *Teoría de la Democracia (2): Los problemas clásicos.* Alianza Universidad (Colección: Ciencias Sociales n.° 567), Madrid, 1987, *Op. cit.* en la p. 373.

[7] Warren era de la aristocracia bostoniana y al casarse empezaron a hacer crónicas ofensivas sobre su vida y sus fiestas, lo que le llevó a realizar un estudio en colaboración con Brandeis que publicaron el 15 de Diciembre de 1890 en *The Harvard Law Review,* cuya conclusión era la siguiente:

> «El derecho consuetudinario ha reconocido siempre a la casa de un hombre como su castillo, inexpugnable, con frecuencia, incluso para sus propios funcionarios ocupados en la ejecución de sus órdenes. ¿Cerrarán así los tribunales la puerta del frente a la autoridad constituida y dejarán abierta la puerta trasera *a la curiosidad ociosa y lasciva?*»

LOTH, D., y ERNST, M. L.: *Control legal de la nueva tecnología.* Marymar, Buenos Aires, 1974, *Op. cit.* en la p. 207.

[8] *Ibidem. Op. cit.* p. 49.

[9] LOTH, D., y ERNST, M. L.: *Control legal de la nueva tecnología,* Marymar, Buenos Aires, 1974, *Op. cit.* en la p. 209.

privada de las personas, no podemos dejar de pensar que era necesaria una legislación[10] sobre el uso incorrecto o irresponsable que se pueda hacer de nuestros datos, ya que no había restricciones legales respecto de ¿quién podía comprar o vender un banco de datos?, no había leyes que obligasen a los propietarios de los bancos de datos a revelar lo que tienen almacenado en sus ordenadores ni a decir cuales han sido sus fuentes de información, en beneficio de la mayoría en cualquier estado suele darse el problema de que el legislativo siempre irá contra la individualidad, etc. El vacío legal era notorio.

Hoy la intimidad, se encuentra inmersa en lo que conocemos como *libertades individuales*[11], o *derechos humanos individuales*, como los llama Diego Gracia Guillén[12], como una parte sustancial de los derechos humanos, a los que habría que añadir los económicos, sociales y culturales que son derechos positivos, es decir los que solamente pueden ser desarrollados por el Estado y, por lo tanto tendrán el valor que éste les quiera conceder, mientras que los derechos individuales son negativos, que son aquellos derechos desarrollados por la iniciativa de los hombres y, por lo tanto, exigibles antes de que se desarrolle una ley para protegerlos. Dentro de estos derechos individuales negativos nos encontramos, además del derecho a la intimidad de las personas, el derecho a la vida, a la salud, a la integridad física, a la libertad, a la propiedad, a la enseñanza, etcétera.

Así pues tenemos tres frentes que requieren una solución para mantener o preservar la confidencialidad de los datos de un individuo dentro de una computadora:

— lo primero es determinar qué es lo que debe ser protegido[13],

---

[10] Los primeros pasos se dieron en Estados Unidos. La Comisión Federal de Comunicaciones inició en el año 1966 una investigación sobre las computadoras, que prosiguió en 1969 y que acabó dando lugar en 1984 a una ley llamada *Privacy Act*, de la que hablaremos más adelante.

[11] Que son «*...todas las pretensiones jurídicas que implican un nexo legal, real o potencial, entre los individuos y el gobierno*» (McCLOSKEY, Robert G.: «Derecho Constitucional: III. Libertades Individuales». En: *Enciclopedia Internacional de las Ciencias Sociales*, dirigida por David L. SILLS, Volumen 3, Aguilar, Madrid, *Op. cit.* en la pág. 546).

[12] Sobre el tema de los derechos humanos, su desarrollo, evolución histórica, repercusiones sociales, etc., hay que leer inevitablemente dos capítulos excelentes de la obra *Fundamentos de Bioética*, Eudema Universidad (Manuales), Madrid, 1989, del citado autor, que son:

— 2. La tradición jurídica y el criterio de autonomía: Los derechos del enfermo (121-198).

— 3. La tradición política y el criterio de justicia: El bien de terceros (199-311).

[13] En cuanto a ¿qué es lo que debe ser protegido? no cabe duda. Hoy se distingue entre *datos personales sensibles* (que son aquellos que no pueden ser tratados automáticamente por un computador en principio, como por ejemplo: datos de carácter médico-sanitario, hábitos sexuales, religión, raza, ideología política, etc.) y *datos personales no sensibles* (que son los que en principio no ofrecen problemas jurídicos a la hora de su informatización. Por ejemplo: nombre, apellidos,

— una vez hecho esto, el segundo paso a dar sería determinar quién debe ser el depositario de esa información[14],
— por último hay que ver cómo podemos preservar esa información.

Los tres puntos son muy importantes pero sólo vamos a ver el tercero de ellos, es decir vamos a analizar el desarrollo de los procedimientos de control para

---

domicilio, teléfono, etc.). En el Proyecto de Ley Orgánica del Tratamiento Automatizado de los Datos de Carácter Personal se prohíben los datos sensibles:

> «... el Consejo de Ministros prohíbe los ficheros creados con la finalidad exclusiva de almacenar datos sensibles e impide que se obligue a declarar sobre ideología, religión y creencias, pero admite que la policía recoja y trate tales datos y los relativos a origen racial o vida sexual cuando "sea absolutamnte necesario para los fines de una investigación concreta". (...), el Gobierno añade ahora, a la denegación del derecho de acceso a los archivos policiales, la denegación a los ficheros de *Hacienda». (PAIS, EL:* «La Ley de informática deniega el acceso a los archivos de la Policía y de Hacienda». *El País,* viernes 28 de junio, 1991, *Op. cit.* en la p. 20.)

En principio esta norma está de acuerdo con al Art. 16.2 de nuestra Constitución que dice *«Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias»* [ADAMS: *La Constitución Española de 1978.* Adams, Madrid, Título I (De los Derechos y Deberes fundamentales), Cap. 2.º (Derechos y Libertades), Sección 1.ª (De los Derechos fundamentales y de las Libertades públicas), 1990, Art. 16.2, *Op. cit.* en la p. 30].

En Estados Unidos la primera referencia legal que nos encontramos en este sentido es la *First Amendment (Primera Enmienda)* que al recoger los conceptos en torno a *«...la libertad de palabra en lo político y en lo religioso, sirvió como principio modélico».* (RUBEN, Brent D.: «En la era de la información: información, tecnología y estudio del comportamiento». *Documentación de las Ciencias de la Información,* 1990, vol. 13, *Op. cit.* en las pp. 61-62) para todas aquellas personas que de una forma u otra nos comunicamos con los demás.

[14] La segunda cuestión que hemos apuntado, ¿quién debe ser el depositario de esa información?, parece que también empieza a dilucidarse jurídicamente pues en todas las leyes se establece un sistema de tutela preventivo para que no sean primero los tribunales los que dictaminen sobre las agresiones contra las libertades informáticas de los sujetos. En la futura Ley Informática Española se pensó en un primer momento en institucionalizar la figura del Comisario de Protección de Datos, similar al Comisario Parlamentario de la Ley del Estado Federal de Hesse o al Data Protection Register de la Data Protection Act del Reino Unido, aunque se ha adoptado la fórmula de Director de la Agencia de Protección de Datos, parecida a la Data Protection Board de los Estados Unidos. Nuestra Agencia *«... actuará con plena independencia de las Administraciones Públicas, pero cuyo director será nombrado por decreto para cuatro años y, aunque no estará sujeto a instrucción alguna, podrá ser separado por el Gobierno, previo expediente. (...), el director de la Agencia de Protección de Datos estará asistido por un Consejo consultivo del que formarán parte representantes de las Administraciones Públicas y de las organizaciones empresariales y de los consumidores, así como expertos (...)».* (PAIS, EL: «La Ley de informática deniega el acceso a los archivos de la Policía y de Hacienda». *El País,* viernes 28 de junio, 1991, *Op. cit.* en la p. 20.)

evitar este tipo de irregularidades, pues los otros dos puntos están más o menos claros en la sociedad actual. Por lo tanto, para preservar la información en un banco de datos tenemos dos opciones:

— medidas físicas para actuar sobre la máquina que guarda esa información confidencial,
— medidas legales para actuar contra quienes atenten contra la seguridad de nuestros datos.

Empezaremos por las medidas físicas de protección de la información.

II. PROTECCION DE LOS DATOS

Hoy contamos con una serie de medidas que garantizan hasta cierto punto la seguridad de la información en un banco de datos:

— el primer sistema de protección de los datos, si vamos desde los medios más sencillos a los más sofisticados, sería el propio soporte que utilizamos para almacenar la información ya que para poder acceder a la información esta tiene que ser leída de alguna forma pues hay que recordar que los datos están codificados y por lo tanto hay que decodificarlos para transformarlos en algo que podamos entender. Desde este punto de vista el soporte tiene que ser legible por un computador para que nosotros podamos acceder a esa información. Este es el caso como ya sabemos de los discos magnéticos, los cassettes o la tarjeta inteligente;
— en segundo lugar, ¿qué podemos hacer con la máquina propiamente dicha? Una medida que se puede emprender sería la puesta a punto de dispositivos mecánicos de protección, como pueden ser el poner al computador, si es que no lo trae de fábrica, una llave de encendido del aparato o una llave de bloqueo del teclado, con lo que se puede ir mejorando la seguridad de los datos almacenados en esa máquina. Pero esta medida no es definitiva por lo que habría que combinarla con otra algo más drástica como puede ser retirar alguno de los componentes vitales para el funcionamiento y puesta en marcha de la máquina, por lo que al carecer de esta pieza no se podrá encender nunca el equipo;
— una tercera medida podría consistir en guardar la información reservada en discos magnéticos removibles, es decir, en discos flexibles o en discos duros externos que después podemos guardar en una caja fuerte. Hasta ahora se puede pensar que hay que trabajar mucho para conservar la información secreta, pero la seguridad informática es un tema serio y delicado que no se puede tomar a la ligera;

— si los dos últimos grupos de medidas hacían referencia al propio computador, vamos a ver ahora desde el punto de vista del software ¿qué podemos hacer para mantener la intimidad de las personas en un banco de datos? Lo primero que se puede hacer es utilizar programas *Compress,* es decir programas que comprimen la información eliminando todo lo que sobra en un fichero y concentrando, por decir de algún modo, los datos que tenga. Esta operación implica después la contraria, es decir, para poder acceder a esta información comprimida hay que descomprimirla antes sino jamás podría ser leída;

— otra medida de software que podemos llevar a la práctica es la utilización de las claves de dígitos (como por ejemplo el *user number* de acceso a bases de datos o las *password*, palabras clave o contraseñas que se utilizan en estos bancos de datos para poder acceder a la información). Hoy cualquier programa de software que utilicemos tiene este sistema de protección y lo único que hay que tener en cuenta es que no seamos ni excesivamente barrocos a la hora de elegirla (pues se nos podría olvidar) ni tampoco excesivamente simples como para denominar a los ficheros que contienen información reservada por ejemplo, *secretos*, *ojo*, *cuidado*, *peligro*, etc., que lo único que hace es reclamar más a los saboteadores;

— también podemos realizar una operación de ocultar la información reservada por medio de una característica del MS-DOS llamada *atributo* que consiste en dar características especiales a los ficheros, como por ejemplo que el fichero sea de solo lectura y por lo tanto no se pueda escribir en él, que sea un fichero oculto, etc. Para que después podamos utilizar estos ficheros habrá que desactivar este comando, lo cual supone un medio más de proteger la información;

— por último podemos utilizar un procedimiento denominado *encriptación* o *criptificación* que consiste en transformar, por medio de claves de codificación, la información que tenemos en un banco de datos en algo que es indescifrable, es decir aplicar procesos determinados a la información para esconderla. Hoy por hoy este método parece que es el que ofrece mayor seguridad aunque la perversión de alguna mente retorcida dará con la forma de saltarse estas medidas.

Hemos visto cómo preservar la confidencialidad de los datos de un individuo dentro de una computadora que era la tercera medida a tener en cuenta en este tema. Ahora vamos a analizar ¿quién debe velar por el desarrollo de los procedimientos de control para evitar este tipo de irregularidades?

III. NIVELES DE CONTROL LEGISLATIVOS

Como es indudable que tenemos la obligación de respetar la intimidad de las personas, hay que procurar los cauces que recojan este derecho del individuo, para lo cual tenemos tres niveles de control establecidos:

— el primer nivel hace referencia a los códigos de ética profesionales, a las tradiciones escritas, a los juramentos y compromisos,
— en un segundo nivel estaría ya la legislación positiva
— por último, en el tercer nivel nos encontramos con las directivas, recomendaciones y reglamentos:

III.a) **Primer nivel**

Dentro de este nivel nos encontramos con el secreto profesional que de alguna manera supondría una forma de protección de los datos de otras personas que pueden estar bajo nuestra custodia en un banco de datos informatizado. Desde los albores de la humanidad sólo tres profesiones eran reconocidas como tales (el sacerdocio, la medicina y el poder judicial) por una serie de condicionantes que no es el momento de explicar. Las tres tenían su secreto profesional, recuerden el secreto de confesión, el secreto sumarial y el secreto médico, estando la información bien guardada, al menos en teoría puesto que «*...el secreto nunca constituye un bien jurídico per se, sino que se trata de un concepto instrumental tras el cual pueden subyacer intereses diversos*»[15], es decir, que puede ser trasgredido en función del bienestar social, por ejemplo. Aún así, sigue siendo una primera medida de tutela de la intimidad personal en los bancos de datos, por lo que va siendo hora de que el secreto profesional sea extensivo a otras profesiones para salvaguardar los datos personales del intrusismo de determinados sujetos o instituciones.

El primer código donde se incluye un artículo que haga referencia al respeto de la confidencialidad informática es el de la Organización Médica Colegial que dice:

> «...los sistemas de informatización médica no *comprometerán el derecho del paciente a la intimidad*»[16].

---

[15] Tal y como opina Fermín Morales Prats, Profesor Titular de Derecho Penal de la Universidad de Barcelona en el artículo de FERNANDEZ, Juan A.: «El secreto profesional médico ante el desarrollo informático». *El Médico: profesión y humanidades*, 11 de mayo, 36-68, 1991, *Op. cit.* en la p. 36.

[16] ORGANIZACION MEDICA COLEGIAL: *Nuevo Código de Ética y Deontología Médica*, marzo, Madrid, 1990, Cap. IV, Art. 19.1.

Pero en lo referente al secreto profesional médico todos sabemos que está bastante devaluado en la actualidad llegando a que algunas Asociaciones Profesionales Médicas reconozcan excepciones al secreto profesional que van desde cuando el paciente consiente a que se pregonen sus datos hasta cuando esos datos son requeridos judicialmente. Por estos motivos, y por los que nos recuerda Morales Prats: «*...la legislación disciplinaria y deontológica no es suficiente para garantizar la tutela de la intimidad...*»[17], hay que procurar que la información esté más protegida por leyes, con lo cual entramos en el segundo nivel.

III.b) **Segundo nivel**

En este nivel de control ya está por medio la ley que siempre suele ser más explícita en sus mandatos y/o prohibiciones. De esta forma tenemos que se recoge este derecho en la Constitución Española de 1978[18] y así en el Art. 18.1 «*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*», y en el Art. 18.4 se dice 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.*» En realidad más que reconocer el derecho a la intimidad de los datos personales, se dice que «*...se limitará el uso de la informática...*» para proteger de alguna forma nuestra intimidad, pero fue un paso importante en el espinoso camino que estamos recorriendo y que se «suavizó» algo más cuatro años más tarde como veremos.

Pero como la confidencialidad de la información de las personas que está contenida en un banco de datos está siempre en peligro de atentados contra ella, estamos obligados a progresar aún más y por este motivo vamos a entrar en el tercer nivel de protección de los datos, dejando para más adelante el tema del desarrollo legislativo que trataremos con más detenimiento.

III.c) **Tercer nivel**

Este nuevo nivel quiza es el más útil de todos pues se trata de una serie de documentos que las instituciones públicas o privadas y las personas físicas elabo-

---

[17] FERNANDEZ, Juan A.: «El secreto profesional médico ante el desarrollo informático». *El Médico: profesión y humanidades,* 11 de Mayo, 1991, Op. cit. en la p. 38.

[18] CONSTITUCION ESPAÑOLA: Título I: De los Derechos y Deberes Fundamentales; Capítulo 2.º: Derechos y Libertades; Sección 1.ª: De los Derechos Fundamentales y de las Libertades Públicas; Artículo 18: Derecho al Honor, la Intimidad y la propia Imagen, 1978.

ran para orientar y dar una serie de recomendaciones que den respuesta a unos supuestos o situaciones determinadas que serían difíciles de resolver por el vacío legal que suele haber en estas materias.

Desde esta perspectiva una recomendación suele hacer referencia a que cada banco de datos tenga su reglamento de funcionamiento según los principios generales más elementales de protección de datos, encontrándonos ya alguna iniciativa en este sentido como la del Comité de Ministros del Consejo de Europa que aprobó el 28 de Enero del año 1981 en Estrasburgo el *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[19], reglamento que fue firmado por todos los países miembros incluida España que lo hizo el 27 de Enero de 1984. Otras iniciativas previas de este organismo internacional fueron:

— la *Resolución sobre la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado* del 26 de Septiembre de 1973,
— la *Resolución sobre la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector público* del 20 de Septiembre de 1974,
— la *Recomendación n.º R (85) 20 relativa a la protección de datos de carácter personal utilizados con fines de marketing directo,*
— la *Recomendación n.º R (86) 1 relativa a la protección de datos de carácter personal utilizados con fines de seguridad social,*
— la *Recomendación del Consejo de Europa sobre Reglamentaciones para bancos informatizados de datos médicos* aprobada el 23 de Enero de 1981,
— la *Recomendación (81/679/CEE) de la Comisión de las Comunidades Europeas, de 29 de Julio de 1981 («DOCE» n.º L 246/31, de 29 de Agosto de 1981), relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal,*
— la *Recomendación relativa a la protección de datos de carácter personal utilizados con fines de investigación científica y estadística* del año 1983,
— o la *Recomendación relativa al SIDA y los derechos del hombre* de 1989 elaborada por la Asamblea Parlamentaria del Consejo de Europa[20].

---

[19] *BOE*: «Convenio para la protección...». *BOE*, n.º 274, 15 de Noviembre, 1985.

[20] Todas estas resoluciones y recomendaciones han sido recopiladas a partir de:
ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* Los Libros de Fundesco (Colección Impactos), Madrid, 1987, 32.

Pero ¿qué dicen estas recomendaciones en concreto? Después de analizarlas y sacando las ideas principales podemos decir que los bancos de datos informatizados que tengan información que se considera reservada:

— deben estar sujetos a las reglamentaciones específicas que en materia de bancos de datos haya en el país de que se trate, acogiéndose por lo tanto a las Leyes del Estado,
— los reglamentos deben ser lo más claros que se pueda para resolver cualquier cuestión que se pueda plantear por el funcionamiento diario de estos bancos de datos
— a pesar de que la información contenida en uno de estos bancos de datos es reservada, hay que dar a conocer públicamente la existencia de los bancos de datos, sobre todo si se va a modificar su estructura o contenidos sustancialmente, cuya finalidad es borrar esa especie de ocultismo que rodea al mundo de la informática en general, y sobre todo para que las personas cuya información se encuentra almacenada dentro de esos bancos de datos conozcan tal eventualidad ya que en la mayoría de las ocasiones el último en enterarse es el propio interesado,
— estas recomendaciones, por regla general contienen una serie de reglas para el buen funcionamiento del banco de datos que podríamos resumir enumerándolas solamente: objetivos y finalidad del banco de datos, tipo de información contenida, persona o institución propietaria del banco de datos, persona o personas que acceden diariamente al banco de datos, persona que supervisa el normal funcionamiento del banco de datos, quién o quiénes pueden introducir, sacar o borrar información, medidas de seguridad de ese banco de datos, etcétera.

Por lo tanto estas recomendaciones, directrices o reglamentos deben procurar respetar escrupulosamente los derechos y las libertades individuales de las personas.

IV. EL RESPETO A LA INTIMIDAD DE LAS PERSONAS: ANALISIS DE LA LEGISLACION ACTUAL

Para concluir esta lección vamos a intentar hacer una recopilación de todo lo que hay fuera de nuestras fronteras y de lo que tenemos aquí referente a la legislación sobre protección de la intimidad de los datos de una persona en un

---

FERNANDEZ, Juan A.: «El secreto profesional médico ante el desarrollo informático». *El Médico: profesión y humanidades,* 11 de Mayo. 1991, 68.

banco de datos. La mayoría de estas leyes protegen a los ciudadanos frente a la intromisión del Estado.

IV.a) Legislación informática en los Estados Unidos de América

A pesar de tener monopolizado buena parte del mercado de los equipos físicos (hardware), de los programas (software) y de la distribución de bases de datos, los norteamericanos que según ellos son los grandes defensores de los derechos humanos no legislaron la protección a la intimidad de las personas en un banco de datos hasta el 31 de Diciembre de 1974, con la *Ley de la Intimidad (The Privacy Act: 5 U.S.C. 552a) de los Estados Unidos de América* que pretendía defender a los ciudadanos de los abusos de los órganos federales de gobierno, pretendía defender los:

«...right of the people to be secure in their persons, *houses, papers, and effects*»[21].

Esta Ley surge poco tiempo después de que aprobaran la Ley de Libertad de Información (*The Freedom of Information Act (5 U.S.C. 552 et seq.)*, también conocida como *FOI Act* o *FOIA*)[22].

Siendo Presidente Gerald Ford, se intentó crear una Agencia para la Protección de los Datos. El Senador Sam Ervin propuso la creación de una especie de Consejo o Tribunal Nacional como parte de la Privacy Act de 1974. La idea fue desechada por el propio presidente. Sin embargo la idea ha sido retomada por Robert E. Wise Jr. representante del partido demócrata de Virginia, que por medio de un Proyecto de Ley dio lugar a que se creara una Comisión que estudiase el caso (*Privacy Protection Study Commission*) que recomendó la creación de la Federal Privacy Board en 1977, como paso previo al establecimientio de la denominada *Data Protection Board*[23].

---

[21] HERNON, Peter, y McCLURE, Charles R.: *Federal Information Policies in the 1980's. Conflicts and Issues*. Ablex Publishing Corporation, New Jersey, 1986, *Op. cit.* en la pág. 66.

[22] Ambas leyes pueden ser estudiadas con más detenimiento en:

— HERNON, Peter, y McCLURE, Charles R.: *Federal Information Policies in the 1980's. Conflicts and Issues*. New Jersey, Ablex Publishing Corporation, 1987 (The Freedom of Information Act 52-66; The Privacy Act 66-82. También pueden verse tratadas estas dos leyes en otras muchas páginas a lo largo de toda la obra).

— McCLURE, Charles R.; HERNON, Peter, y RELYEA, Harold C.: *United States Government Information Policies. Views and Perspectives*. New Jersey, Ablex Publishing Corporation, 1989 (The Freedom of Information Act 46-47, 125, 130-131 and 172; The Privacy Act 36, 43-44, 88, 117, 172 and 299).

[23] ROTENBERG, Marc: «In Support of a Data Protection Board in the United States». *Goverment Information Quarterly*, 1991, vol. 8 n.º 1, 79-93.

En 1984 publicaron la *Counterfeit Access Device and Computer Fraud and Abuse Act* (Ley sobre artificios de acceso falseado y fraude y abuso informáticos) que trata sobre el acceso a los datos, su utilización y destrucción que recortaba las competencias federales en esta materia, y en el 86 la *Electronic Communication Privacy Act* que respondía a las necesidades de defensa de la privacidad en las nuevas formas de comunicación.

En Canadá, que introducimos en este epígrafe pues no tiene cabida en el siguiente, nos encontramos la *Criminal Law Amendement Act* de 20 de Junio de 1985 que es una ley que hace más hincapié en la protección de los sistemas informáticos, pero que toca aspectos concretos de la protección de los datos automatizados. De todos modos los Canadienses se adhirieron a las *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* de 1980. Esta normativa nace en la O.C.D.E. (Organización de Cooperación y Desarrollo Económico) y tiene como principios básicos de aplicación los siguientes:

— interrelación con los principios básicos de la práctica informativa,
— establecimiento de unos stándares mínimos de aplicación (calidad de los datos, limitaciones de uso, medidas de seguridad, participación de los ciudadanos, etc.),
— las medidas adoptadas en la normativa pueden ser complementadas con medidas de protección adicionales[24].

IV.b) **Legislación informática en la Comunidad Económica Europea**

La primera fue una *Ley Regional del Estado Federal de Hesse* de Octubre de 1970, región que se encuentra en el centro de la República Federal Alemana, que protegía al ciudadano de las agresiones del Estado por medio de un Comisario Parlamentario de Protección de Datos que tenía que velar por el cumplimiento de la ley en relación a la protección de la intimidad de las personas. Esta figura venía a ser parecida al Defensor del Pueblo en nuestro país. Esta ley de todos modos no tenía recogidas ningún tipo de sanciones.

El segundo país donde se empieza a ver la necesidad de legislar estos temas fue Suecia, y así el 11 de Mayo de 1973 aprueban en su parlamento la *Data Act*

---

[24] Se puede ampliar este tema en:

POTVIN, Louise: «Privacy Issues in the Information Age: What Corporations Need to Know». *Goverment Information Quarterly*, 1991, vol. 8, n.º 1, 95-99.

LESSER, Barry: «Information Protection Issues in the Information Economy». *Bulletin of the American Society for Information Science*, February/March, 1988, 21-22.

(Ley de Datos), que a diferencia de la anterior ya contempla la posibilidad de sancionar civil y penálmente a los infractores. Nueve años más tarde se modificó la Sección 21 de esta Ley introduciendo un nuevo articulado que tipificaba el delito de acceso indebido a los datos[25].

En tercer lugar fueron los Estados Unidos de América los que elaboraron una Ley tal y como hemos visto en el párrafo anterior, siendo nuevamente Alemania pionera en leyes de este tipo y el 27 de Enero de 1977 aprueban la *Ley Alemana Federal de Protección de Datos* que ya contempla la figura jurídica del manipulador de datos y contiene una serie de infracciones penales y administrativas muy rigurosas.

Pero además de leyes que penalicen a los infractores nos encontramos otras que empiezan a recoger otros aspectos legales como es por ejemplo regular de alguna forma la creación de bancos de datos. El ejemplo lo tenemos en Francia que en 1978 aprueba la *Loi d'Informatique et des Libertés* que dio lugar a la creación de una Comisión Nacional de Informática y Libertades que es la que tiene que aprobar la creación o la modificación de los bancos de datos que hay en el país. Además están intentando reformar el Código Penal para introducir artículos que traten el tema de la utilización fraudulenta de los sistemas de tratamiento automático de la información[26].

Pero sin duda la ley más importante elaborada en el Reino Unido y la primera que verdaderamente limitaba los posibles perjuicios ocasionados a las personas por el abusivo uso que se está haciendo de los datos personales informatizados fue la *Ley de Protección de Datos (Data Protection Act)* de 1984, por lo que vamos a detenernos brevemente en su análisis.

La *Data Protection Act* se limita solamente a datos[27] personales, debiendo cumplir cuatro exigencias:

---

[25] «*Any person who unlawfully procures access to a recording for automatic data processing or unlawfully alters or obliterates, or enters such a recording in a file shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years, unless the offence is punishable under the Penal Code.*»

ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*. Los Libros de Fundesco (Colección Impactos), Madrid, 1987, *Op. cit.* en la p. 97.

[26] Esto podemos constatarlo en DEVEZE, Jean: «La fraude informatique. Aspects juridiques». *La Semaine Juridique*, n.º 3.289, 1987.

[27] Que define como la «*...información que se registra en una forma que se puede procesar por el equipo que funciona automáticamente en respuesta a las instrucciones dadas para tal propósito*» [CLAYTON, Marlene: *Gestión de automatización de bibliotecas*. Fundación Germán Sánchez Ruipérez (Colección: Biblioteca del Libro), Madrid, 1991, *Op. cit.* en la pág. 265.]

— la ley especifica que datos personales deben almacenarse y las utilizaciones que se van a hacer de ellos,
— no se puede divulgar la información contenida salvo que el interesado esté de acuerdo en ello,
— debe de quedar registrada toda institución o persona física, pública o privada que inscriba datos personales
— y, por último, todas las personas sobre las que se han reunido los datos deben ser informadas de que, al menos, esa información existe.

Pero además hay unos principios que deben ser asumidos por cualquier persona que manipule este tipo de información. Estos principios son los siguientes:

1.° Los datos personales recogidos deben ser exactos, sin errores y se manipularán de la misma forma.
2.° Los datos personales se recogerán para un fin previamente especificado y de acuerdo con la ley.
3.° Haciendo hincapié con el punto anterior, los datos personales solamente se utilizarán para la finalidad propuesta en un principio.
4.° Se recogerán los datos necesarios (adecuados y pertinentes) para el propósito estipulado.
5.° Los datos personales hay que actualizarlos siempre y cuando sea necesario.
6.° Siempre se establecerá un tiempo de utilización de los datos recogidos en función de la finalidad para la que fueron recopilados.
7.° Las personas a las que se refieren los datos recopilados tienen derecho a: conocer que se está reuniendo información sobre ellas, acceder a esos datos, corregir o eliminar los datos que considere oportuno, y
8.° Hay que adoptar todas las medidas de seguridad física y lógica que podamos para evitar el acceso de personas no autorizadas, la alteración voluntaria o involuntaria de la información recogida, la divulgación de la información o la destrucción, y consiguiente pérdida de los datos provocada o inconscientemente. Estos principios deben ser cumplidos en su totalidad, estableciendo para ello un sistema de vigilancia que se denomina *Data Protection Register*, es decir, una serie de normas que debe cumplir la persona que se encarga de registrar los datos. Estas normas[28] son las siguientes: a) mantener actualizada toda la informa-

[28] Que fueron desarrolladas por LIBRARY ASSOCIATION (The) en la obra *Data Protection and the Library and Information Community: Some Guidelines for Policy, Iniciatives and Practices*. London, 1985.

ción sobre bancos de datos: datos que contienen, usuarios de los mismos, creador del banco, etc.; b) garantizar que todos los datos cumplen los principios que hemos enumerado anteriormente y que son utilizados de acuerdo a la ley; c) divulgar en los foros pertinentes los contenidos y principios de la ley; d) estudiar cualquier demanda interpuesta por el mal uso de los datos personales o por cualquier infracción de la ley; y e) controlar la actividad de los usuarios así como proceder cuando se cometan infracciones.

Para concluir con la *Data Protection Act*, que estamos desarrollando más detenidamente pues es una ley importante, hay que señalar que cada vez que se tenga previsto realizar una recogida de datos para crear un banco de datos personales, la ley prevee que la o las personas que vayan a realizar esta tarea deben informar por escrito de tal eventualidad al *Data Protection Register* en los siguientes términos:

— nombre y dirección de los recopiladores de datos,
— enumeración de los datos que se van a recopilar,
— información detallada de los usos y finalidad de ese banco de datos,
— fuentes que se van a utilizar para reunir los datos,
— enumeración de las personas sobre las que se piense difundir información,
— enumeración de los países donde se piensa mandar esa información,
— direcciones donde se solicita la utilización o acceso a esos datos.

Es una forma de proteger la intimidad de las personas pues las implicaciones criminales en las que uno se puede ver envuelto, por utilizar información contenida en bancos de datos de formas distintas a las expuestas en el registro de entrada del *Data Protection Register*, son ilimitadas.

IV.c) **Otros tipos de regulaciones**

En nuestro país lo más reciente en torno al tema que estamos abordando, tenemos que en el año 1982 se publica la *Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*[29].

Posteriormente se edita una *Orden de 30 de Julio de 1982 sobre limitación de acceso a la información contenida en las bases de datos fiscales*[30].

Fuera de nuestro país pero en nuestro entorno socio-económico-político-cultural, tenemos que hablar de la Comunidad Económica Europea, pues este

[29] BOE: «Ley Orgánica 1/1982...». *BOE*, n.º 115, 14 de Mayo, 1982.
[30] BOE: «Orden de 30 de Julio...». *BOE*, n.º 190, 10 de Agosto, 1982.

apartado se quedaría corto si no hablásemos de la Protección de Datos en el Mercado Unico Europeo, es decir, ¿qué hace la CEE al respecto? Todo lo que hemos visto hasta ahora han sido iniciativas particulares de algunos países de la Comunidad, pero la CEE ha emprendido una serie de acciones para que sean cumplidas por todos los países miembros, y que pretenden erradicar los posibles abusos de mal uso de los datos personales sobre todo por la transferencia de información que se puede producir hoy en día gracias a las telecomunicaciones y a las redes de computadores.

El 18 de Julio de 1990 una Comisión del Consejo de Europa (*Data Protection Commission*) redactó un Comunicado que incluía seis propuestas sobre las que había que empezar a trabajar en diversas Subcomisiones para elevar el nivel de protección de los datos personales almacenados de forma automática. Estas propuestas de trabajo a desarrollar a corto plazo, fueron las siguientes[31]:

- una *Directiva* dirigida al establecimiento en la Comunidad de un nivel elevado de protección de datos basada en el *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* aprobado por el Comité Europeo de Ministros el 28 de Enero del año 1981 en Estrasburgo
- una *Recomendación* de adhesión de los países miembros al Convenio del Consejo de Europa,
- una *Resolución* con vistas a extender la protección a los ficheros de datos personales del sector público,
- una *Declaración* donde se recogerán los principios de protección de los datos personales guardados o recogidos por los cuerpos o instituciones comunitarias,
- una *Directiva Sectorial* con vistas a adaptar los principios generales de la protección de datos a las necesidades específicas de las aplicaciones telemáticas de cada país, para establecer unos stándares legales de homogeneización de las tecnologías,
- una *Decisión* en el campo de la seguridad de los sistemas de información ante la vulnerabilidad de los mismos.

Estas estrategias que persigue la Comisión Europea se desarrollarán en varias fases habiendo en cada una de ellas unas líneas de investigación prioritarias, pero se

[31] Esto está recogido en un artículo anónimo de dos páginas que es «Protection of Personal Data in a Single Market». *I'M. Information Market Issue n.º 64*. September/October 1990. Published by Directorate General XIII: Telecommunications, Information; Industries and Innovation, Commission of the European Communities, Luxembourg; 1-2.

trata al menos de una línea de trabajo que tenderá a armonizar criterios y elaborar una serie de medidas que al ser asumidas por los países de la CEE harán que éstos al menos tengan una política común en algo tan importante como es la protección de la intimidad de los datos personales almacenados en medios automatizados[32].

Pero no acaba aquí la legislación informática europea. Hay artículos dentro de determinadas leyes que aluden a la protección de los datos automatizados. Veamos algunos ejemplos[33]:

— La *Constitución de Portugal* del año 1976 dice en su Art. 35:

> «1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos. 3. Queda prohibida la atribución de un *número nacional único a los ciudadanos*»[34].

Además hay varios artículos del Código Penal de 1982 donde se tipifican algunas acciones delictivas relacionadas con la informática (Art. 181, 229.2, 230 y 231), y por último el *Proyecto de Ley sobre Protección de Datos* de 15 de Marzo de 1984.

— La *Segunda Ley para la Lucha contra la Delincuencia Económica* de la República Federal Alemana (15 de Mayo de 1986) dio lugar a importantes modificaciones en el Código Penal Alemán, apareciendo artículos rela-

---

[32] Como no podemos detenernos por más tiempo en estos aspectos tan puntuales, recomendaremos la lectura de los artículos que enumeramos a continuación para todos aquellos que quieran profundizar más en los trabajos de esta Comisión, así como para ver ¿qué temas se trataron en el 12th. Annual World Data Protection Commissioners Meeting celebrado en París:

RILEY, Tom: «International Privacy Developments». *ACCESS Reports*, September 19, 1990, 7-9

— «Special Report: International Developments». *ACCESS Reports*, January 4, 1990, 9-12.

— «Special Report». *ACCESS Reports*, April 4, 1990, 6-10.

— «Special Report: Data Protection War in the Offing». *ACCESS Reports*, October 3, 1990, 6-11.

— «Special Report». *ACCESS Report*, December 12, 1990, 7-10.

[33] Que están ampliamente desarrollados en ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*. Los Libros de Fundesco (Colección Impactos), Madrid, «Las Tendencias Legislativas en el Derecho Comparado», 1987, 90-106.

[34] ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*. Los Libros de Fundesco (Colección Impactos), Madrid, 1987, *Op. cit.* en la p. 28.

tivos a: espionaje de datos (Art. 202 a), alteración de datos (Art. 303 a), sabotaje informático (Art. 303 b), etcétera[35].

— La *Ley n.º 229 de 6 de Junio de 1985 (Ley de modificación del Código Penal: Delincuencia Informática)* de Dinamarca, incluye un artículo acerca del tema que estamos tratando (Art. 279 a).
— *Proyecto Ministerial de modificación del Código Penal* de Austria (1985) en su Art. 147a.
— *Proyecto de Ley para el reforzamiento de la lucha contra la criminalidad económica y el fraude informático* de Luxemburgo en su Art. 496.
— La *Theft Act* del Reino Unido (1968) es otra ley que como en los casos anteriores lo que intenta es tipificar de algún modo las figuras delictivas que están surgiendo de la manipulación incorrecta, en todas sus formas, de los datos personales de cada uno de nosotros que por uno u otro motivo se encuentran almacenados en un banco de datos, siendo las características más importantes de todas ellas las siguientes:

a) todas las leyes están concebidas para ser aplicadas sobre bancos de datos públicos o privados informatizados, por lo que se excluyen los ficheros manuales,
b) las leyes tutelan solamente los datos personales. El resto de datos que pueda haber en un banco de datos quedan fuera de estas jurisdicciones,
c) en cada una de las leyes se establecen las pautas de control preventivas (autorizaciones, licencias, Data Protection Register, etc.) para impedir los atentados contra la intimidad personal,
d) por detrás de estos sistemas de tutela preventivos se encuentran siempre los tribunales de justicia que entrarán en acción cuando la infracción se haya cometido y los controles preventivos han sido incapaces de establecer las penas y multas pertinentes,

---

[35] Uno de los más explícitos es el Art. 263 a, que dice lo siguiente:

> «El que, con la intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, lesiona el patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta del programa, la utilización incorrecta o incompleta de datos, la utilización de datos sin autorización, o la intervención de cualquier otro modo no autorizado en el proceso, será castigado con la pena de privación de libertad de hasta cinco años o con *multa*.»

ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información*. Los Libros de Fundesco (Colección Impactos), Madrid, 1987. *Op. cit.* en la p. 92.

e) también establecen la leyes las pautas de seguridad necesarias para el caso en que los datos personales sean *sensibles* que, aunque está prohibido recogerlos siempre hay excepciones,
f) todas las leyes establecen las condiciones de manipulación de los datos,
g) por último, todas las leyes establecen los cauces y permisos necesarios para intercambiar información con otros países (lo que se viene llamando *flujo transfronterizo de datos*) y los países con los que se puede y no intercambiar esa información.

Vamos a pasar ahora a analizar como está la situación en nuestro país, siempre en esa doble vertiente de la protección de los datos y la propiedad de las herramientas que tratan automáticamente esos datos.

V. EL CASO ESPAÑOL

V.a) **Código civil**

Son muy escasas las normas que nos encontramos en el Código Civil[36], además de que no hacen referencia a la protección de los datos. Así en el Libro II nos encontramos con dos Artículos sobre la Propiedad Intelectual, el 428 que dice «*El autor de una obra literaria, científica o artística, tiene el derecho a explotarla y disponer de ella a su voluntad*» y el 429 que se refiere a que «*La ley sobre la propiedad intelectual determina las personas a quienes pertenece ese derecho, la forma de su ejercicio y el tiempo de su duración. En casos no previstos ni resueltos por dicha ley especial, se aplicarán las reglas generales establecidas en este Código sobre la propiedad*»[37], y en general un articulado sobre los bienes y la propiedad aunque no hace una alusión expresa a la propiedad de los datos personales confidenciales que se encuentran almacenados en las bases de datos que hay en el país.

Pero en 1982 se dio un paso importante para garantizar la protección civil de este derecho, nos estamos refiriendo a la *Ley Orgánica 1/1982 de 5 de Mayo sobre la Protección Civil del Derecho al Honor, a la Intimidad Personal y Fami-*

---

[36] Hemos manejado la edición del BOE: Código Civil. *Boletín Oficial del Estado* (Serie Universitaria), 2.ª ed. de junio de 1984, Madrid.

[37] Capítulo III (De la propiedad intelectual); Título IV (De algunas propiedades especiales); Libro II (De los bienes, de la propiedad y de sus modificaciones) del *Código Civil*, *BOE* (Serie Universitaria), Madrid, 1984, *Op. cit.* en la p. 430

liar y a la propia Imagen, que apareció en el *BOE*, n.º 115 de 14 de mayo de 1982. No hay ninguna alusión concreta a la informática pero podemos entender que en los artículos 7.3 y 7.4[38] no sería incorrecto el contemplar la informática como una de las formas de tener almacenados los datos personales y poder utilizarla para difundir los mismos, por lo que caería dentro de la tutela jurídica de esta ley.

V.b) **Código penal**

En cuanto al *Código Penal Español*[39] hay varios artículos que hacen referencia a la intimidad de las personas pero sin tipificar claramente el delito en relación a las bases de datos (Artículos: 192 bis[40], 360[41], 367 y 368 que hacen referencia a la revelación de los secretos e informaciones privilegiadas y de su

---

[38] Dicen así:

— Art. 7.3: «*La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.*»

— Art. 7.4: «*La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.*»

[Ley Orgánica 1/1982 de 5 de mayo sobre la Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen: Cap. II (De la Protección Civil del Honor, de la Intimidad y de la Propia Imagen), Art. 7.º (De las Intromisiones Ilegítimas). En: BOE: *Código de Legislación Informática. Boletín Oficial del Estado*. Madrid, 1988, 42-45].

[39] Hemos utilizado la edición preparada por DIAZ-MAROTO y VILLAREJO, Julio, y SUAREZ GONZALEZ, Carlos J.: *Código Penal y Legislación Complementaria*. Civitas (Biblioteca de Legislación), 16.ª ed. actualizada a septiembre de 1991, Madrid, 1991.

[40] Dice así este artículo:

> «La Autoridad, funcionario público o agente de éstos que sin la debida autorización judicial, salvo en su caso lo previsto legalmente en desarrollo del artículo 55.2 de la Constitución, interceptare las comunicaciones telefónicas o utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido incurrirá en la pena de arresto mayor en su grado máximo e inhabilitación absoluta.
>
> Si divulgare o revelare la información obtenida por cualquiera de los precitados medios, se le impondrá la pena inmediatamente superior en grado a la prevista en el párrafo anterior.»

[41] Este artículo se expresa en los siguientes términos:

> «Será castigado con las penas de suspensión y multa de 100.000 a 500.000 pesetas el Abogado o Procurador que, con abuso malicioso de su oficio, o negligencia o ignorancia inexcusable, perjudicare a su cliente o descubriere sus secretos, habiendo tenido conocimiento de ellos en el ejercicio de su profesión.»

incorrecto uso[42], 497, 498 y 499 que se refieren al descubrimiento y revelación de secretos[43]). No obstante el *Proyecto de Reforma del Código Penal* de 1980 y

[42] El primero de estos artículos dice:

> «El funcionario público o autoridad que revelare los secretos o cualquier información de que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados será castigado con las penas de suspensión y multa de 100.000 a 200.000 pesetas.
>
> Si de la revelación a que se refiere el párrafo anterior resultare grave daño para la causa pública o para tercero, las penas serán de prisión menor e inhabilitación especial.
>
> Si se tratare de secretos de un particular, las penas serán las de arresto mayor, suspensión y multa de 100.000 a 500.000 *pesetas.*»

En cuanto al Art. 368, dice así:

> «El funcionario público o autoridad que, haciendo uso de un secreto de que tenga conocimiento por razón de su oficio o cargo, o de una información privilegiada, obtuviere un beneficio económico para sí o tercero, será castigado con las penas de inhabilitación especial y multa por el importe del valor del beneficio obtenido o facilitado. Si resultare grave daño para la causa pública o para tercero, las penas serán las de prisión *menor e inhabilitación especial.*
>
> A los efectos de este artículo, se entiende por información privilegiada toda información de carácter concreto que se tenga exclusivamente por razón de oficio o cargos públicos y que no haya sido notificada, publicada o divulgada.»

[43] El 497 dice:

> «El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las *penas de arresto mayor y multa de 100.000 a 2,000.000 de pesetas.*
>
> Si no los divulgare, las penas serán de arresto mayor y multa de *100.000 a 500.000 pesetas.*
>
> Esta disposición no es aplicable a los padres, tutores o quienes hagan sus veces en cuanto a los papeles o cartas de sus hijos o *menores que se hallen bajo su dependencia.*»

El Artículo 498 sigue en la misma línea que el anterior:

> «El administrador, dependiente o criado que en tal concepto supiere los secretos de su principal y los divulgare será castigado con las penas de arresto mayor y multa de 100.000 a *500.000 pesetas.*»

Por último, el 499 dice:

> «El encargado, empleado u obrero de una fábrica u otro establecimiento industrial que en perjuicio del dueño descubriera los secretos de su industria será castigado con las penas de arresto mayor y multa de 100.000 a 1,000.000 de pesetas.»

la *Propuesta de Anteproyecto de Nuevo Código Penal* de 1983 ya hace referencia expresa a los delitos informáticos. Así por ejemplo, el Art. 189 de la Propuesta de Anteproyecto incluye los atentados informáticos contra la intimidad:

> «1. El que, infringiendo las prescripciones legales sobre el uso de la informática, grabare datos relativos al honor o a la intimidad personal o familiar de terceros, o en perjuicio de los mismos manipulare la información legítima o ilegítimamente obtenida, será castigado con la pena de arresto de doce a veinticuatro fines de semana y multa de seis a doce meses, siempre que el hecho no constituya delito más grave. 2. Se impondrán las penas superiores en grado si se divulgare la *información obtenida*»[44].

Substancialmente algo avanza este artículo pero aún nos parece insuficiente pues nos remite a una ley que hay que desarrollar todavía y porque además establece una conducta prohibitiva escasamente sancionada.

VI. CONCLUSIONES

Concluiremos diciendo que una Ley sobre el uso de la Informática se está haciendo necesaria[45]:

1.º una ley que recogiese de algún modo las iniciativas que se están llevando a cabo en todos los países que hemos estudiado, que a primera vista parece que están más desarrollados que nosotros en este aspecto legislativo que podemos achacar, no a una mayor tradición democrática, sino tal vez a que ellos han utilizado con mucha mayor antelación que nosotros esta herramienta tecnológica nueva,

2.º una ley en la que no solamente se proteja al individuo de las agresiones del Estado o de otras personas naturales o jurídicas, sino también donde el ciudadano pueda tener acceso a sus propios datos para conocer la información que puede haber almacenada en un banco de datos y controlar, de alguna manera el uso que se está haciendo de sus propios datos por otras personas o instituciones tanto públicas como privadas,

3.º una ley que impida el que llegue a ser realidad la profecía de George

---

[44] ROMEO CASABONA, Carlos M.ª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* Los Libros de Fundesco (Colección Impactos), Madrid, 1987, *Op. cit.* en la p. 30.

[45] En la actualidad hay un anteproyecto de ley informática que tiene que pasar a discutirse en el Parlamento Español (*Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales*).

Orwell[46], es decir una ley que impida la marginación del tipo que sea de una persona por el mero hecho de que sus datos personales almacenados en una computadora puedan ser fácilmente obtenidos por cualquier persona o institución, pública o privada,

4.° una ley para que sea el ciudadano el que regule la tecnología, y no los gobiernos o las grandes empresas, pues la regulación «*...es uno de los pocos medios del ciudadano para ejercer su influencia*»[47] sobre la sociedad.

BIBLIOGRAFIA SOBRE DELITO INFORMATICO

I. **Monografías**

ADAMS (1990): *Constitución Española de 1978*. Madrid, Centro de Estudios ADAMS,

BIRKINSHAW, Patrick (1988): *Freedom of Information*. Weidenfeld, London.

BOE (1984): *Código Civil*. Madrid, *Boletín Oficial del Estado* (Serie Universitaria).

BOE (1988): *Código de legislación informática*. Madrid, *Boletín Oficial del Estado*.

BONDIA ROMAN, F. (1988): *Propiedad intelectual: su significado en la sociedad de la información. La Nueva Ley de 11 de Noviembre de 1987*. Trivium, Madrid.

BUREAU OF NATIONAL AFFAIRS (1989): *Computer Data Security: a Legal and Practical Guide to Liability, Loss Prevention, and Criminal & Civil Remedies*. Washintong, Bureau of National Affairs.

CAMACHO LOSA, Luis (1987): *El delito informático*. Gráficas Cóndor, Madrid.

CEBRIAN, Juan Luis y *cols.* (1988): *El secreto profesional de los periodistas*. Centro de Estudios Constitucionales (Colección: *Cuadernos y Debate*, n.° 12), Madrid.

CLAYTON, Marlene (1991): «La Ley de Protección de Datos». En: CLAYTON, Marlene: *Gestión de automatización de bibliotecas*. Fundación Germán Sánchez Ruipérez, Madrid, 265-271.

[46] Orwell concibió un modelo de sociedad en la que existiría un *Hermano Mayor* que, como tal hermano conocería todo lo relativo a las personas emparentadas con él directa o indirectamente, para utilizarlo según le conviniera. Gracias a la intrusión de las computadoras en la sociedad que nos ha tocado vivir, el hermano mayor podría ser el gobierno, las compañías de crédito, la patronal, las asociaciones de índole político, religioso, ideológico, etc. que quieran curiosear en los datos personales de cada uno de nosotros que se encuentren en los bancos de datos. La profecía de Orwell puede analizarse con más detenimiento en LOTH, David, y ERNST, Morris L.: «La Ley y la Computadora», Cap. 17 de la obra *Control Legal de la Nueva Tecnología* de los mismos autores. Marymar, Buenos Aires, 1972, 203-217.

[47] Palabras debidas a Rose y que son citadas por RUBEN, Brent D.: «En la era de la información: información, tecnología y estudio del comportamiento». *Documentación de las Ciencias de la Información*, 1990, vol. 13, en la p. 63.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (1985): *5ème. Rapport d'activité de la Commission (1983-1984).* París.

COUNCIL OF EUROPE (1985): *Beyond 1984: the Law and Information Technology in Tomorrow's Society.* Strasbourg, Council of Europe.

DELGADO PORRAS, A. (1988) *Panorámica de la protección civil y penal en materia de propiedad intelectual.* Civitas, Madrid (Colección: Biblioteca de Legislación).

DENNINGER, Erhard (1987): «El derecho a la autodeterminación informativa». En: PEREZ LUÑO, Antonio Enrique: *Problemas actuales de la documentación y la informática jurídica.* Tecnos, Madrid, 268-274.

DESANTES, José María (1987): *Teoría y régimen jurídico de la Documentación.* EUDEMA, Madrid.

DIAZ-MAROTO y VILLAREJO, Julio, y SUAREZ GONZALEZ, Carlos J. (1991): *Código Penal y Legislación complementaria.* Civitas, Madrid (Colección: Biblioteca de Legislación).

FISHER, Royal P. (1988): *Seguridad en los sistemas informáticos.* Díaz de Santos, Madrid.

FLAHERTY, David H. *et all.* (1984): *Privacy and Data Protection: an International Bibliography.* Knowledge Industry Publications.

FLAHERTY, David H. *et all.* (1989): *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and The United States of America.* North Carolin University Press.

FREDBARG, Birgit, y PIEYNS-RIGO, Paulette (1988): *Les consèquences juridiques de la production des documents informatiques par les administrations publiques.* UNESCO, París.

FROSINI, Vittorio (1987): «Problemas jurídicos de la información y documentación». En: PEREZ LUÑO, Antonio Enrique: *Problemas actuales de la documentación y la informática jurídica.* Tecnos, Madrid, 49-80.

FUNDESCO (1986): *Formación de técnicos e investigadores en tecnologías de la información. Análisis de la oferta y la demanda de estos profesionales en España.* Fundesco, Madrid (Colección: Estudios y Documentos).

GERBNER, George; GROSS, Larry P., y MELODY, William H. (eds.) (1973): Communications Technology and Social Policy: Understanding the *New Cultural Revolution.* John Wiley & Sons, New York.

GRACIA GUILLEN, Diego (1989): *Fundamentos de Bioética.* EUDEMA Manuales, Madrid.

GREENWOOD, Gareth (1984): *Códigos y claves secretas. Criptografía en BASIC.* Anaya Multimedia, Madrid.

HERNON, Peter, y McCLURE, Charles R. (1987): *Federal Information Policies in the 1980's. Conflicts and Issues.* Ablex Publishing Corporation, New Jersey.

JOHNSON, Deborah (1985): *Computer Ethics.* Englewood Cliffs, New Jersey.

KALBHEN, Uwe; KRUCKEBERG, Fritz, y REESE, Jürgen (1983): *Las repercusiones sociales de la tecnología informática*. Fundesco/Tecnos, Madrid.

KIRBY, M. D. *et all.* (1983): *An Exploration of Legal Issues in Information and Communications Technologies*. París, Organisation for Economic Cooperation and Development.

LAVER, Murray (1983): «Intimidad y protección de datos». En: LAVER, Murray: *Los ordenadores y el cambio social*. Fundesco/Tecnos, Madrid.

LOTH, David, y ERNST, Morris L. (1974): «Aire para las comunicaciones». En: LOTH, David, y ERNST, Morris L.: *Control legal de la nueva tecnología*. Ediciones Marymar, Buenos Aires (Argentina), 113-123.

— (1974): «La ley y la computadora». En: LOTH, David, y ERNST, Morris L.: *Control legal de la nueva tecnología*. Ediciones Marymar, Buenos Aires (Argentina), 203-217.

MARETT, P. (1991): *Information Law and Practice*. Gower, Aldershot.

McCLURE, Charles R.; HERNON, Peter, y RELYEA, Harold C. (1989): *United States Government Information Policies. Views and Perspectives*. Ablex Publishing Corporation, New Jersey.

MILLARD, Christopher J. (1985): *Legal Protection of Computer Programs and Data*. Carswell, Toronto (Canada).

MILLER, Arthur R. (1971): *Assault on Privacy: Computers, Data Banks and Dossiers*. Michigan University Press, Ann Arbor.

MINISTERIO DE TRANSPORTES, TURISMO Y COMUNICACIONES (1988): *Ley de ordenación de las telecomunicaciones*. MTTC, Madrid.

MOLINERO, C. (1989): *Teoría y fuentes del derecho de la información*. Promociones y Publicaciones Universitarias, Barcelona.

PEINADO BENAYAS, M.ª del Carmen (1989): *Aplicaciones sociales de las nuevas tecnologías de la información en España*. Fundesco (Colección Informes), Madrid.

PEREZ LUÑO, Antonio Enrique (1989): «Los derechos humanos en la sociedad tecnológica». En: LOSANO, Mario G.: *Libertad informática y leyes de protección de datos personales*. Centro de Estudios Constitucionales, Madrid, 133-185.

— (1987): *Nuevas tecnologías, sociedad y derecho: el impacto socio-jurídico de las nuevas tecnologías de la información y la comunicación*. Fundesco (colección impactos), Madrid.

— (1987): *Problemas actuales de la documentación y la informática jurídica*. Tecnos, Madrid.

PRESIDENCIA DE GOBIERNO (1977): *Leyes de protección de datos*. Ministerio de la Gobernación, Madrid.

RIVERO, A. M., y SANTODOMINGO, A. (Eds.) (1986): *Introducción a la informática jurídica*. Fundesco (Colección Impactos), Madrid.

RODRIGUEZ PRIETO, Antonio (1986): *Protección de la información. Diseño de criptosistemas informáticos*. Paraninfo, Madrid.

ROMEO CASABONA, Carlos (1987): *Poder informático y seguridad jurídica. La función tutelar del Derecho Penal ante las Nuevas Tecnologías de la Información*. Fundesco (Colección Impactos), Madrid, 25-34.

SLOAN, Irving J. (1986): *Law of Privacy Rigths in a Technological Society*. Oceana Publications.

TANEMBAUM, A. (1985): «Seguridad de los sistemas de archivos». En: — *Sistemas Operativos*. Osborne/McGraw-Hill, Madrid, 295-315.

THOMAS, A. J., y DOUGLAS, I. J. (1988): *Auditoría informática*. Paraninfo, Madrid.

VARIOS AUTORES: «Derecho». En: David L. Sillis (dir.): *Enciclopedia Internacional de las Ciencias Sociales*. Aguilar, Madrid, vol. 3, 502-605.

VARIOS AUTORES (1989): *Información y libertades públicas en España*. Universidad Complutense de Madrid (Cursos de Verano de El Escorial), Madrid.

WILSON, Alexander (1988): *Library Policy for Preservation and Conservation in the European Community. Principles, Practices and the Contribution of New Information Technologies*. Strasbourg: Commission of the European Communities.

YEARBOOK of Law Computers and Technology. Leicester Polytechnic Press, vol. 1 (s.d.).

II. **Publicaciones seriadas**

ADNEY, William M., y DAVANAGH, Douglas E.: «Los bandidos de datos». *Byte*, 1989, enero 86-88.

BERGANTINE, F. (1989): «La seguridad informática». *Mundo Científico*, 26, 1983, Junio, 676-686.

BOSHIER, Roger (1990): «Socio-Psychological Factors in Electronic Networking». *International Journal of Lifelong Education*, vol. 9, n.º 1, 49-64.

BRAHAMS, Diana, y WYATT, Jeremy (1989): «Decision Aids and the Law». *The Lancet*, 8663, september 632-634.

CEE (1990): «Protection of personal data in a Single Market». *I'M. Information Market*, 64, 1-2.

«COMPUTERS and Privacy. The Eye of the Beholder». *The Economist*, may 4, 1991, 21-23.

CUADRA, Bonifacio (de la) (1991): «La Ley de Informática». *El País*, viernes 28 de junio, 1-20.

DESANTES GUANTER, José M.ª (1978): «Derecho de la Información e Información del Derecho». *Documentación de las Ciencias de la Información*, n.º II, 21-23.

— (1981): «Problemas jurídicos de la documentación informativa». *Documentación de las Ciencias de la Información*, n.º V, 223-241.

FERNANDEZ, Juan A. (1991): «El secreto profesional médico ante el desarrollo informático». *El Médico: profesión y humanidades*, 11 de mayo, 37-68.

FUNDESCO (1988): «Sanidad y nuevas tecnologías de la información. Aspectos jurídicos». *Cuadernos de FUNDESCO*, 6, Madrid 1-67.

GONZALEZ BEDOYA, Jesús (1981): «Etica de la Información: Repertorio bibliográfico y temático». *Documentación de las Ciencias de la Información*, n.º V, 83-222.

GRAIÑO, Alvaro (1990): «Lucha contra los piratas: tras la tregua comenzará la ofensiva». *PC WEEK*, Noviembre 71, 14-22.

ISBELL, Mary K. (1986): «Confidentiality of Online Bibliographic Searches: Attitudes and Practices». *RQ*, vol. 25, n.º 4, 483-487.

LESSER, Barry (1988): «Information Protection Issues in the Information Economy». *Bulletin of the American Society for Information Science*, February/March, 21-22.

LEWIS, Peter H. (1991): «Why the Privacy Issue Will Never Go Away». *The New York Times*, Sunday April 7.

MITCHAM, C. (1988): «Ética profesional en las altas tecnologías». *Conferencia pronunciada en INVESCIT*, Valencia, 9 de Noviembre de 1988.

MILLION, Angela, y FISHER, Kim N. (1986): «Library Records: A Review of Confidentiality Laws and Policies». *Journal of Academic Librarianship*, vol. 11, n.º 6, 346-349.

MORAN, J. M., y BOTANA, H. (1990): «Protección de la información». *El Médico, profesión y humanidades*, Mayo 63-64.

PC-MAGAZINE (1990): «Sólo para sus ojos: ficheros privados en un PC compartido». *PC-MAGAZINE*, n.º 31, 351-374.

PESO NAVARRO, Emilio (del) (1990): «Auditoría informática como medio de prevención del delito informático». *ALI*, 23-26.

POTVIN, Louise (1991): «Privacy Issues in the Information Age: What Corporations Need to Know». *Government Information Quarterly*, vol. 8, n.º 1, 95-99.

RAMOS GONZALEZ, M. A. (1990): «Auditoría informática e ingeniería del conocimiento». *ALI*, 39-43.

RILEY, Tom (1990): «International Privacy Developments». *Access Reports*, September 19, 7-9.

— «Special Report: International Developments». *Access Reports*, 1990, January 4, 9-12.

— «Special Report». *Access Reports*, 1990, April 4, 6-10.

— «Special Report: Data Protection War in the Offing». *Access Reports*, 1990, October 3, 6-11.

— «Special Report». *Access Report*, 1990, December 12, 7-10.

ROTENBERG, Marc (1991): «In Support of a Data Protection Board in the United States». *Government Information Quarterly*, vol. 8, n.º 1, 79-93.

RUBEN, Brent D. (1990): «En la era de la información: información, tecnología y estudio del comportamiento». *Documentación de las Ciencias de la Información*, vol. 13, 53-72.

SANCHEZ GONZALEZ, Miguel (1990): «Informática Médica: Problemas éticos y legislativos (I, II, III, IV y V)». *El Médico, profesión y humanidades*, Septiembre/Octubre, 49-50; 73-74; 87-88; 77-78 y 109-110.

SANTESMASES, M.ª J., y MARTIN PALLIN, J. A. (1989): «Poderes y derechos de la informática». *El Independiente*, 8 de Octubre, 10-11.

SCHIRMACHER, Wolfgang (1986): «Privacy as an Ethical Problem in the Computer Society». *Philosophy and Technology*, II.

SHAVER, Donna B. *et al.* (1985): «Ethics for Online Intermediaries». *Special Libraries*, vol. 76, n.º 4, 238-245.

«TITLE 5: Government Organization and Employees». *Pub. L.*, 1966, September 6, 449-462.

USHERWOOD, Robert (1990): «Ethics of Information». En: *Institute of Information Scientists (Proceedings of the Annual Conference)*, 1989, 4-7 July Harrogate. Edited by Jennifer E. Rowley in «Where the Book Stops. The Legal Dimensions of Information», London, 93-101.

VARIOS AUTORES (1990): «Bioética». *Bol. Of. Sanit. Panam.*, vol. 108, n.º 5/6 (Número Especial) Mayo/Junio, 369-652.

VARIOS AUTORES (1989): «Filosofía de la Tecnología. Una Filosofía Operativa de la Tecnología y de la Ciencia». *ANTHROPOS*, n.º 94/95, 1-128.

VARIOS AUTORES (1989): «Poderes y derechos de la informática». *El Independiente*, 8 de Octubre, 10-12.

WILSON, K. y *cols.* (1983): «¿Qué informática necesita la ciencia?». *Mundo Científico*, Octubre, 29, 1042-1048.

ZAPATERO GOMEZ, Victorino Félix: «Seguridad de acceso al ordenador». *ALI*, 49-51.