El respeto a la intimidad de las personas: análisis de la legislación actual

Carlos Manuel DA COSTA CARBALLO*
Isabel PORTELA FILQUEIRAS**
Inmaculada CEBRIAN DOMINGUEZ***

I. Introducción

En el Vol. 2 Nº 1 de la Revista General de Información y Documentación esbozamos, bajo el título de "Algunas cuestiones éticas y jurídicas sobre documentación automatizada", parte de la normativa que hay hoy en día vigente en algunos países acerca del siempre delicado tema de la protección de los datos personales almacenados en los bancos de datos informatizados. Si tenemos en cuenta que no hicimos un estudio exhaustivo de las mismas, además de que con posterioridad se promulgó la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, el lector comprenderá el ¿por qué? de retomar nuevamente este tema tan importante.

Vamos a intentar hacer una recopilación de todo lo que hay en el terreno legislativo fuera de nuestras fronteras y de lo que tenemos aquí referente a la protección de la intimidad de los datos de una persona en un banco de datos. La mayoría de estas leyes protegen a los ciudadanos frente a la intromisión del Estado.

Los motivos de este punto creo que están bastante claros después de lo que acabamos de comentar unas líneas más arriba, pero por si todavía hace falta alguna razón de mayor peso el Art. 6º de nuestro Código Civil es bastante explícito al respecto: "...la ignorancia de las leyes no excusa de su cumplimiento"[1].

* Profesor de Biblioteconomía y Documentación. E.U.B.D. Complutense
** Profesora Ayudante EUBD Complutense
*** Licenciada en Geografía e Historia

[1] Art. 6.1. Cap. III (Eficacia general de las normas jurídicas), Títulos Preliminar (De las normas jurídicas, su aplicación y eficacia) [B.O.E.: *Código Civil*. Madrid: Boletín Oficial del Estado (Serie Universitaria), 1984. Op cit en la pág. 23].

No cabe duda de que lo que acabamos de leer pudiera parecernos excesivo en el sentido de que si solamente hubiera normas emanadas de la Administración Central del Estado podría ser factible estar más o menos enterado de las mismas, pero si tenemos en cuenta que además están las de las Comunidades Autónomas, las de las Comunidades Europeas, etc., etc., esto es prácticamente imposible. No obstante aquí vamos a repasar que nos encontramos en este terreno tan delicado.

Empezaremos por los Estados Unidos, incluyendo en este epígrafe a Canadá.

II. Legislación informática en América del Norte

II.a. Estados Unidos de América

Coincidiendo en el mes y año con la promulgación de la Ley de Protección de Datos del Land de Hesse aunque 19 días más tarde, en los Estadios Unidos de América se desarrolla el Fair Reporting Act (26 de Octubre de 1970) con la que se pretendía auxiliar a unos ciudadanos muy particulares (los clientes de las entidades de crédito) que veían alterado su derecho a la intimidad en manos de las agencias informativas. Tenía una ventaja innegable y es que era de aplicación a datos personales almacenados en cualquier tipo de soporte, pero tenía un gran inconveniente que no la hacía ser una ley muy operativa, que era el que debía ser el ciudadano que considerase que sus derechos habían sido vulnerados el que recurriese a los tribunales de justicia para reclamar la reparación de sus perjuicios, es decir, de esta forma era el ciudadano el que ejercía un control indirecto de sus derechos.

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"[2]. ¿Por qué?. Porque la "Privacy is the right of individuals to control to disclosure of personal information and to hold those accountable who misuse information, breach a confidence, or who profit from the sale of information without first obtaining the consent of the individual. In the design of a computer system containing personal information, it is a pri-

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

mary consideration"[3]. Es decir, se trata de un derecho que tenemos para poder controlar la divulgación de nuestros datos, así como la venta de los mismos sin nuestro consentimiento. Así expresado parece que la persona al dar su consentimiento está dispuesta para recibir una gratificación, y en este juego tampoco debe caerse. Si consideramos que nuestros datos no deben utilizarse para determinados fines, no deben utilizarse bajo ningún concepto ni mediando una gratificación o similar. Quizás sea esta una postura muy tajante, pero yo pienso que no es ético exigir la protección de un derecho al que nosotros mismos estaríamos dispuestos a renunciar si mediase algún tipo de compensación.

Esta Ley, The Privacy Act, 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)[4].

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). La Comisión inició entonces un estudio acerca de la protección de datos que concluyó en 1977 con la recomendación de la creación de una Agencia Federal de la Privacidad (The Federal Privacy Board), como paso previo al establecimiento de la denominada Data Protection Board[5].

El informe final de este estudio, que puede seguirse en el artículo citado de Marc Rotenberg, constaba de cuatro puntos cuyas ideas principales son:

- continuar las investigaciones acerca de este tema
- establecer la implementación de unos estatutos y recomendaciones
- revisión del acta de privacidad de 1974
- exponer las regulaciones que adoptasen al Presidente, Congreso, Gobierno, etc.

---

[3] Rotenberg, Marc: "In Support of a Data Protection Board in the United States". *Goverment Information Quarterly* (1991) Vol. 8 Nº 1. Op cit en la pág. 80.

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

- Hernon, Peter and 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 and 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].

[5] Rotenberg, Marc: "In Support of a Data Protection Board in the United States". *Goverment Information Quarterly* (1991) Vol. 8 Nº 1 79-93.

The Privacy Act es una ley muy amplia de la que vamos a sacar aquellos puntos más importantes para los fines que perseguimos.

La ley inicia su exposición con una serie de definiciones, como por ejemplo ¿qué es un registro?, ¿qué son registros estadísticos?, ¿qué es un programa de ordenador?, etc., etc. La más interesante, sin despreciar el resto de definiciones, es la del registro que viene a ser una agrupación o colección de datos relativos a una persona. A continuación la ley establece las condiciones en que debe de hacerse la divulgación de los datos personales contenidos en un sistema automatizado y ¿cómo puede accederse a esa información?. Prosigue con una serie de normas para mantener la información registrada en un sistema automatizado, las reglas de funcionamiento, los deberes y derechos de los depositarios oficiales de esa información y las "multas" por incumplir esa normativa, 5.000 $ por difundir datos en virtud de su situación laboral o por obtener información bajo falsas finalidades no contempladas en las reglas generales de funcionamiento del sistema[6], aunque también hay excepciones generales y especiales, que ocupan los dos apartados siguientes. También habla de los archivos de registros, de los acuerdos entre las partes y de los informes bianuales que deben realizar todas las agencias de protección de datos personales ubicadas en los Estados Unidos de América, tanto las federales como la nacional):

> *"(s) Biennial report*
> *The President shall biennially to the Speaker of the House of Representatives and the President pro tempore of the Senate a report*
> *(1) describing the actions of the Director of the Office of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;*
> *(2) describing the exercise of individual rights of access and amendment under this section during such years;*

---

[6] *"(i) Criminal penalties*
(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5.000.
(2) Any officer or employee of an agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5.000.
(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5.000"
["TITLE 5: Government Organization and Employees". *Pub. L.* (1988) September 6 449-462. Op cit en la pág. 453].

(3) identifying changes in or additions to systems of records;
(4) containing such other information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out purposes of the Privacy Act of 1974"[7].

Hay más puntos en esta Ley que no vamos a tratar por no extendernos excesivamente en cada una de las que estamos analizando, pero vamos a concluir diciendo que se trata de una normativa que pretende defender a las personas en base a que la intimidad o privacidad de los datos en un derecho fundamental que todos tenemos en la mayoría de los países, y desde luego los norteamericanos no dejan dudas sobre esto[8].

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.

También en 1984 desarrollaron The Cable Communications Policy Act que prohibía los servicios de divulgación de información por cable, salvo que hubiese consentimiento por parte de la persona de la que se mandaban los datos. Dos años más tarde la Asociación del Correo Electrónico (The Electronic Mail Association), después de varios estudios realizados sobre la protección de datos en el correo electrónico, consigue que se haga una Ley que proteja esto de alguna manera (The Electronic Communication Privacy Act)[9].

En el año de 1988 promulgan otra Ley (The Computer Matching Act) para prevenir el excesivo desarrollo que se estaba produciendo en la elaboración de dossiers automatizados, y por lo tanto el más que probable intercambio de datos personales entre las compañías sobre todo del sector privado[10].

---

[7] "TITLE 5: Government Organization and Employees". Pub. L. (1988) September 6. Op cit en la pág. 455.

[8] Baste, para finalizar, esta cita tan clara y expresiva que es innecesario comentar:
"The right to privacy is a personal and fundamental right protected by the Constitution of de United States; and in order to protect the privacy of individuals identified in information systems maintaained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies"
["TITLE 5: Government Organization and Employees". *Pub. L.* (1988) September 6. Op cit en la pág. 458].

[9] Esta Ley de 1986 prohibe la interceptación de mensajes mandados por medio de esta tecnología, define todo lo relativo a comunicaciones electrónicas (correo electrónico, transmisiones vía satélite, telefonía celular, etc), establece las sanciones civiles y penales por infringir la normativa, etc.

[10] Rotenberg, Marc: "In Support of a Data Protection Board in the United States". *Goverment Information Quarterly* (1991) *Vol. 8 Nº 1* Op cit en la pág. 88.

Como esta legislación sólo tiene aplicación en el caso de la administración federal, cualquier problema que se suscita en cuanto a la protección de datos es analizado desde la óptica de las Normas para la Protección de los Movimientos Secretos y Traspasos de los Datos Personales promulgadas por la OCDE, que aunque sólo son recomendaciones han servido para que determinadas empresas y asociaciones dicten una serie de medidas que llenen el vacío legal que existe en estos temas.

II.b. Canadá

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 en 1984 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[11].

Se definen los datos personales y el flujo transfronterizo de datos, los primeros como aquella información relativa a un individuo identificable, lo segundo como el movimiento o trasbase de datos personales a través de las fronteras[12].

Estas normas representaron el primer intento de proteger los datos personales así como un fomento del flujo de datos entre los pueblos aunque de forma reglada. Además tenía un punto bastante positivo, al menos desde mi punto de vista, y es que estas normas se concibieron para ser aplicadas tanto a datos personales automatizados como manuales.

---

[11] Se puede ampliar este tema en:

- Potvin, Louise: "Privacy Issues in the Information Age: What Corporations Need to Know". *Government Information Quarterly* (1991) Vol. 8 Nº 1 95-99.
- Lesser, Barry: "Information Protection Issues in the Information Economy". *Bulletin of the American Society for Information Science* (1988) *February/March* 21-22.

[12] *"Personal data is any information relating to an identifiable individual"*

y

"Transborder flows is defined as movements of personal data across national borders"

[Potvin, Louise: "Privacy Issues in the Information Age: What Corporations Need to Know". *Government Information Quarterly* (1991) *Volume 8 Number* 1 95-99. Op cit en la pág. 95].

Se dividían en dos partes llamadas ambas principios básicos, aunque unos eran de aplicación nacional y otros internacional. En los Basic Principles of National Application se establecieron los estándares mínimos de protección de datos aunque, como hemos comentado unas líneas anteriores, siempre podían suplirse con medidas adicionales. Establecieron los límites a las "colecciones de datos personales" en el sentido de que sólo había que recopilar los datos imprescindibles de cada persona y los más relevantes: "Personal data should be relevant to the purposes for which they are to be used"[13]. Como veremos en otras normas se recomendaba también utilizar los datos para las finalidades de recopilación de los mismos, y no para otros menesteres. Promovía una serie de medidas encaminadas a establecer una seguridad mínima en cuanto a accesos no autorizados, destrucción de datos, modificaciones, etc. Crea la figura del controlador de datos y establece los cauces legales para que las personas puedan acceder a sus datos.

En cuanto a los Basic Principles of International Application desarrollaron todos los puntos concernientes al flujo de datos[14].

III. Legislación informática en la Comunidad Económica Europea

Hemos visto en el artículo citado al comienzo de esta exposición en que consiste el derecho a la intimidad. De todos modos, y en relación a los bancos de datos donde pueden estar nuestros datos personales, creo que no estará de más recordar brevemente que el right to privacy es la conjunción de los siguientes derechos:

- derecho de acceso a los bancos de datos
- derecho de control de la exactitud de los datos
- derecho de puesta al día de los datos recopilados
- derecho de rectificación de los datos
- derecho de secreto para los datos sensibles, si es que han sido recogidos
- derecho de autorización para la difusión de nuestros datos.

Vamos a analizar ahora cómo los diferentes países de la Comunidad Económica Europea intentan salvaguardar estos derechos que acabamos de enumerar.

---

[13] Potvin, Louise: "Privacy Issues in the Information Age: What Corporations Need to Know". Goverment Information Quarterly (1991) Volume 8 Number 1. Op cit en la pág. 96.

[14] Como no podemos entretenernos excesivamente con cada norma que estamos enumerando, sobre las Guidelines on the Protection... debe consultarse el trabajo citado de Louise Potvin.

III.a. República Federal Alemana

La primera legislación al respecto fue una Ley Regional del Estado Federal de Hesse de 7 de Octubre de 1970, llamada Ley de Protección de Datos (Datenschutzgesetz). El Land de Hesse es una región que se encuentra en el centro de la República Federal Alemana. Desarrolló la primera normativa que protegía al ciudadano de las agresiones del Estado por medio de un Comisario Parlamentario de Protección de Datos (Datenschutzbeauftragter) 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 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.

En 1978 se promulga el Acta Federal para la Protección de Datos Personales y contra el uso indebido del Procesamiento de Datos de aplicación en ambos sectores sociales, el público y el privado. La figura jurídica del Comisario de Datos tiene distintas competencias en función de la institución en la que desarrolle su labor. Así, hay un Comisario Federal de Datos (Deutschen Bundespost) que vela por el cumplimiento de la normativa en las administraciones públicas en todo el territorio federal, y 12 Comisarios Estatales con sus respectivas Agencias Estatales de Protección de Datos para cada uno de los Estados de la República Federal que se encargan del sector privado. Ahora con la unificación no cabe duda de que esto variará substancialmente.

En la actualidad se está desarrollando una enmienda a la Ley Federal de Protección de Datos para dar cobertura legal al problema del flujo transfronterizo de datos que no era contemplado en la legislación mencionada.

Esto en cuanto a datos personales almacenados en bancos de datos. ¿Qué sucede con los datos que entran a formar parte de cualquier servicio de telecomunicación?.

El 1 de Enero de 1988 se redactan las Regulaciones para las Telecomunicaciones (Telekommunikationsordnung) donde se encuentran una serie de medidas generales de aplicación en determinados servicios, como por ejemplo:

- utilización de los datos personales para elaboración de informes
- utilización de los datos personales para el establecimiento de las comunicaciones
- utilización de los datos personales para las tareas de facturación de servicios

- prohibición de revelar los datos de cualquier persona
- establecer las medidas de seguridad oportunas para proteger los datos[15].

En general como dice HansPeter Gebhadt "La mayoría de estas disposiciones están basadas en el concepto que se tiene de que los datos pueden emplearse, exclusivamente, para los objetivos de las telecomunicaciones, y que los mismos deben borrarse luego de un determinado tiempo;..."[16].

III.b. Suecia

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 (Ley de Datos), que a diferencia de la anterior ya contempla la posibilidad de sancionar civil y penálmente a los infractores. Para ello los encargados de la protección de datos, Swedish Data Inspection Board, tienen competencias a la hora de desarrollar las regulaciones oportunas con respecto a la seguridad de los datos.

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[17].

En el año 1984 el Parlamento sueco crea la Comisión para la Protección de la Privacidad Personal en las Sociedades de la Información cuyas competencias son muy similares a las del Data Protection Register, Comisión Nacional de Informática y Libertades, Data Protection Board, etc., por lo que no vamos a incidir más en estos detalles.

III.c. Francia

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, Ley 78/17 de 6 de Enero, que dio lugar a la creación de una

[15] Estas regulaciones que acabamos de mencionar se encuentran en la sección 84 párrafo 1; sección 105 párrafo 2.3 y sección 108 párrafo 1 [Informes anuales del Comisario Federal para la Protección de Datos Nº 7-10 (1985-87) recogidos por J. Schmidt].

[16] Gebhardt, Hans-Peter: "La protección de datos en países desarrollados. Principios y situación jurídica". *Telos: Cuadernos de Comunicación, Tecnología y Sociedad* (1989) Nº 18 Junio/Agosto Op cit en la pág. 134.

[17] *"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 Mª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* Madrid: Los Libros de Fundesco (Colección Impactos), 1987. Op cit en la pág. 97].

Comisión Nacional de Informática y Libertades (C.N.I.L.) 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[18].

Esta ley del país vecino concede unos poderes casi ilimitados a la C.N.I.L. e impone unas penas bastante rigurosas a quien incumpla las normas.

En el otro ámbito de protección, las telecomunicaciones, Francia ha adoptado varias resoluciones de interés que comentaremos brevemente. En 1983 decidieron omitir los cuatro últimos números de los teléfonos de los usuarios de este tipo de servicios a la hora de pasarles los recibos pertinentes, o a la hora de utilizar aparatos que registran los números de los abonados que utilizan este tipo de servicios. Se prohibieron los aparatos de llamada automática hasta que no se implantaran medidas de seguridad oportunas. Esto sucedió en 1985. Dos años más tarde, 1987, se prohibieron las promociones de marketing telefónico porque "Se consideró que el ser molestado frecuentemente con llamadas telefónicas que tienen el propósito de un marketing representaba una violación a la privacidad"[19].

Otra medida muy interesante desde la perspectiva de usuarios que todos somos por unos u otros motivos, ha sido la creación de una especie de listado donde cada uno puede inscribirse si no desea que le manden propaganda de marketing telefónico. Este listado ha sido denominado liste orange.

Por último, en cuanto al correo electrónico, la C.N.I.L. estableció unas directrices el 12 de Abril de 1988 que voy a transcribir por su importancia:

> *"- la no inscripción en el directorio del buzón electrónico debe ser gratuita;*
>
> *- el abonado debe recibir de France Télécom una contraseña personal cuando solicita el servicio;*
>
> *- el abonado puede rechazar los mensajes de personas que no estén abonadas al servicio;*
>
> *- se introducen medidas técnicas de manera*
>
> *que*
>
> ** el abonado tenga la posibilidad de averiguar cualquier uso no autorizado de su contraseña;*

[18] Esto podemos constatarlo en Deveze, Jean: "La fraude informatique. Aspects juridiques". *La Semaine Juridique* (1987) Nº *3289*.

[19] Gebhardt, Hans-Peter: "La protección de datos en países desarrollados. Principios y situación jurídica". *Telos: Cuadernos de Comunicación, Tecnología y Sociedad* (1989) Nº 18 Junio/Agosto Op cit en la pág. 131.

** se desapruebe la búsqueda sistemática de ciertas contraseñas"* [20].

Esto es lo más importante de la normativa que hemos podido manejar acerca de la protección de datos en la República Francesa.

III.d. Reino Unido

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[21] personales, debiendo cumplir cuatro exigencias:

- 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:

1º Los datos personales recogidos deben ser exactos, sin errores y se manipularán de la misma forma.

2º Los datos personales se recogerán para un fin previamente especificado y de acuerdo con la ley.

3º Haciendo hincapié con el punto anterior, los datos personales solamente se utilizarán para la finalidad propuesta en un principio.

4º Se recogerán los datos necesarios (adecuados y pertinentes) para el propósito estipulado.

5º Los datos personales hay que actualizarlos siempre y cuando sea necesario.

---

[20] Gebhardt, Hans-Peter: "La protección de datos en países desarrollados. Principios y situación jurídica". *Telos: Cuadernos de Comunicación, Tecnología y Sociedad* (1989) *Nº 18* Junio/Agosto Op cit en la pág. 132.

[21] 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*. Madrid: Fundación Germán Sánchez Ruipérez (Colección: Biblioteca del Libro), 1991. Op cit en la pág. 265].

6º Siempre se establecerá un tiempo de utilización de los datos recogidos en función de la finalidad para la que fueron recopilados.

7º 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.

8º 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[22] son las siguientes: a) mantener actualizada toda la información 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 infor-

[22] Que fueron desarrolladas por THE LIBRARY ASSOCIATION en 1985 en la obra *Data Protection and the Library and Information Community: Some Guidelines for Policy, Iniciatives and Practices* editada en Londres.

mación contenida en bancos de datos de formas distintas a las expuestas en el registro de entrada del Data Protection Register, son ilimitadas.

Por último, en cuanto a los servicios de telecomunicación lo más significativo que nos encontramos en el Reino Unido es la obligación de variar la contraseña asignada a los usuarios de los servicios de videotex.

III.e. Suiza

También en este país centroeuropeo se han dado cuenta de la gravedad del vacío legal en cuanto a la protección de datos. De esta forma, en 1983 se desarrolló un Proyecto de Ley Federal sobre la Protección de Datos que se encuentra en tramitación parlamentaria desde 1988.

No hemos podido conseguir el texto de este anteproyecto pero según la fuente citada[23] y haciendo referencia a las telecomunicaciones, el Art. 16 "...no permite que aparezca información alguna en los extractos acerca de los nombres, direcciones o números de teléfono de los abonados", términos muy similares a los que hemos visto en otras normativas.

IV. Otros tipos de regulaciones

El marco en el que se van desarrollando las normativas que veremos a continuación, han cambiado notablemente con respecto al que había cuando surgieron las primeras leyes de protección de datos (Hesse, Suecia, etc.), por lo que creo que sería conveniente empezar enumerando las características o factores desencadenantes de estas nuevas normativas. ¿Cuáles han sido estos factores desencadenantes de las nuevas leyes?:

- en primer lugar, el cambio que se ha producido en la gestión de los sistemas informáticos, pasando de unos sistemas centralizados a otros distribuidos o descentralizados
- el espectacular avance de la microinformática
- el no menos espectacular aumento de las capacidades de memoria de los ordenadores así como el incremento de velocidad de proceso de los equipos
- la entrada del procesamiento automático de datos en todas las esferas sociales: laboral, educativa, etc.
- el conflicto establecido entre la consecución de unos derechos fundamentales y las necesidades de información demandada por la sociedad

[23] Gebhardt, Hans-Peter: "La protección de datos en países desarrollados. Principios y situación jurídica". *Telos: Cuadernos de Comunicación, Tecnología y Sociedad* (1989) *Nº 18* Junio/Agosto Op cit en la pág. 130.

- las necesidades de seguridad de los sistemas informáticos como consecuencia de la mala praxis derivada del uso de estos equipos
- el cambio producido en la acepción de los datos para informar a datos para comercializar
- la asunción de la libre circulación de información en el mercado único europeo, lo cual repercute también sobre los datos personales, etc.

Este entorno ha dado lugar a que se empiece a hablar de leyes de 2ª generación (lo que nosotros hemos llamado en otra parte de este trabajo como tercer nivel de control legislativo) frente a las otras leyes (Hesse, Suecia, etc.) que por ser las primeras que surgieron se han quedado clasificadas como leyes de 1ª generación. Es de las de 2ª generación de las que nos vamos a ocupar en este momento.

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[24].

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[25].

Indirectamente, el Art. 20.1 de nuestra Carta Magna[26] guarda relación con el tema de la protección de datos que estamos tratando en el sentido de que el apartado a) recoge la protección del derecho de libertad de expresión, mientras que el apartado d) se refiere a las garantías del derecho, no menos importante, a la información. De todas formas tendríamos que desviarnos bastante del rumbo que nos hemos marcado al iniciar este seminario por lo que no vamos a continuar por este camino en estos momentos[27].

---

[24] B.O.E. (1982): "Ley Orgánica 1/1982..."; *B.O.E.*; *Nº 115*; 14 de Mayo

[25] B.O.E. (1982): "Orden de 30 de Julio..."; *B.O.E.*; *Nº 190*; 10 de Agosto

[26] *"1. Se reconocen y protegen los derechos:*
a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
b) A la producción y creación literaria, artística, científica y técnica.
c) A la libertad de cátedra.
d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades".
[Adams: *La Constitución Española de 1978*. Madrid: Adams, 1990. Art. 20; Sección 1ª (De los derechos fundamentales y de las libertades públicas); Cap. II (Derechos y libertades); Título I (De los derechos y deberes fundamentales); Pág. 32].

[27] Sólo comentaré para concluir que en otras dos Constituciones se recogían aspectos similares al que acabamos de comentar. Estas eran:
- Art. 40 de la Constitución de Yugoslavia que se refería al establecimiento de garantías para que las emisiones fueran veraces y objetivas y, por lo tanto de interés para la sociedad, y el
- Art. 48.2 de la Constitución Portuguesa que viene a decir que todos los integrantes de la sociedad, tanto los sujetos de forma individual como las instituciones públicas o privadas, tienen derecho a ser con-

Fuera de nuestro país pero en nuestro entorno socio-económico-político-cultural, tenemos que hablar de la Comunidad Económica Europea, pues este apartado se quedaría corto si no hablásemos de la Protección de Datos en el Mercado Unico Europeo, es decir, ¿qué hace la C.E.E. al respecto?. Todo lo que hemos visto hasta ahora han sido iniciativas particulares de algunos países de la Comunidad, pero la C.E.E. ha emprendido una serie de acciones para que sean cumplidas por todos los países miembros, y que pretenden erradicar los posibles abusos del 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.

Comenzaremos por el Convenio 108 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. Este Convenio tiene tres partes bien diferenciadas:

1: principios básicos

2: normativas sobre datos transfronterizos

3: mecanismos de ayuda recíproca entre las partes

Lo que nos interesa en este momento son los principios básicos pues sobre ellos es sobre los que se deben desarrollar las legislaciones de protección de datos que se elaboren en la C.E.E. Estos principios básicos son los siguientes[28]:

- obtención de los datos que van a formar parte de un banco de datos de forma legal, informando a los interesados para obtener su consentimiento
- establecer claramente la finalidad que se persigue con la creación de un banco de datos personales
- toma de datos con una gran exactitud
- adecuar los datos tomados a los fines del banco de datos

---

venientemente informados tanto por el gobierno como por cualquier otra autoridad de la gestión que se lleve a cabo en cualquier asunto público de interés general.

Para profundizar más en este tema hay que consultar la siguiente obra: Sánchez Férriz, Remedios: "Las libertades de expresión y de información y los derechos al honor, a la intimidad y propia imagen". En: *Información y libertades públicas en España*. Madrid: Universidad Complutense (Cursos de Verano de El Escorial, 1989), 1990 [173-194].

[28] Sólo vamos a enumerarlos ya que cualquier persona interesada en un desarrollo más profundo debe consultar:

- B.O.E.: "Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal, hecho en Estrasburgo el 28 de Enero de 1981". En: B.O.E.: *Código de Legislación Informática*. Madrid: Boletín Oficial del Estado, 1988 (27-41).

- B.O.E.: "Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal, hecho en Estrasburgo el 28 de Enero de 1981". *Boletín Oficial del Estado* (1985) *Nº 274* 15 de Noviembre.

- Velázquez Bautista, Rafael: "Protección de datos personales: Convenio 108 del Consejo de Europa y la Propuesta de directiva de la CE". *Boletín de la Fundación para el Desarrollo de la Función Social de las Comunicaciones* (1992) *Nº 128* Abril 10-12.

- pertinencia de los datos para la finalidad establecida
- conservación de los datos mientras que estos sean útiles a la finalidad establecida
- establecimiento de los derechos fundamentales de acceso a un banco de datos por parte del interesado, derecho a rectificar sus datos y derecho a eliminar o cancelar los datos que quiera
- establecimiento de las excepciones a la norma de forma clara y concisa
- regular las formas de recurso contra los infractores o contra quienes nos impidan u obstaculicen alguno de los derechos que acabamos de enumerar.

Visto de forma tan breve el Convenio 108, vamos a analizar a continuación las otras medidas que ha emprendido la C.E.

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[29]:

- 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.

---

[29] 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 Nº 64*; September/October 1990; Published by Directorate General XIII: Telecommunications, Information; Industries and Innovation; Commission of the European Communities; Luxembourg; 1-2

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 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 C.E.E. 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[30].

Sin embargo en estas normativas encontramos también puntos débiles. Por ejemplo: se diferencia excesivamente entre ficheros públicos y privados, cuando la norma debería ser idéntica para ambos. Además en los ficheros del sector público hay una serie de excepciones que debilitan, al menos en mi opinión, bastante la defensa de la intimidad de las personas. Las instituciones creadas para controlar el cumplimiento de la ley (Agencia de Protección de Datos, Data Protection Register, etc.) no tienen asignadas unas competencias claras ni tampoco tienen una independencia total para ejercer su tarea sin levantar suspicacias o recelos. Algunas de estas normativas, por ejemplo nuestro Anteproyecto (la LORTAD), no establece grandes medidas de seguridad para los datos y para su transmisión por medios telemáticos, por lo que cabe pensar que se van a producir bastantes anomalías en el flujo transfronterizo de datos.

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[31]:

- 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

[30] 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* (1990) September 19 7-9.
- Riley, Tom: "Special Report: International Developments". *ACCESS Reports* (1990) January 4 9-12.
- Riley, Tom: "Special Report". *ACCESS Reports* (1990) April 4 6-10.
- Riley, Tom: "Special Report: Data Protection War in the Offing". ACCESS Reports (1990) October 3 6-11.
- Riley, Tom: "Special Report". *ACCESS Report* (1990) December 12 7-10.

[31] Que están ampliamente desarrollados en Romeo Casabona, Carlos Mª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* Madrid: Los Libros de Fundesco (Colección Impactos), 1987. Ver: "Las Tendencias Legislativas en el Derecho Comparado"; 90-106.

prohibida la atribución de un número nacional único a los ciudadanos"[32].

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.

- En el año 1978, en el Land de Renania del Norte-Westfalia, se modificó el Art. 4º de su Constitución para introducir el reconocimiento del derecho a la protección de los datos ("Datenschutz"), de la misma forma que han hecho algunos estados norteamericanos en sus respectivas constituciones (como por ejemplo: Washington, Florida, California, Iowa, Arizona, etc.[33]).
- 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 relativos a: espionaje de datos (Art. 202 a), alteración de datos (Art. 303 a), sabotaje informático (Art. 303 b), etc.[34].
- La Ley Nº 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).

---

[32] Romeo Casabona, Carlos Mª: *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información.* Madrid: Los Libros de Fundesco (Colección Impactos), 1987. Op cit en la pág. 28. El artículo originariamente dice:

"1. Todos os cidadaos têm o direito de tomar conhecimento do que constar de registros mecanográficos a seu respeito e do fim a que se destinam as informaçoes, podendo exigir a rectificaçao dos dados e a sua actualizaçao.

2. A informática nao pode ser usada para tratamento de dados referentes a convicçoes políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados nao identificáveis para fins estatísticos.

3. É proibida a atribuçao de um número nacional único aos cidadaos"

[*CONSTITUÇAO da república portuguesa.* Lisboa: Impresa Nacional Casa da Moeda, 1976. Art. 35 (Utilizaçao da informática); Título II (Direitos, liberdades e garantias); Parte I (Direitos e deveres fundamentais); Pág. 29].

[33] Esta información puede ser ampliada en las siguientes obras:

- Heredero, Manuel: "La informática y el uso de la información personal". En: VARIOS AUTORES: *Introducción a la informática jurídica.* Madrid: Fundesco (Colección: Impactos), 1986 33-46.

- López Bustos, Francisco Luis y López-Sidro Jiménez, Luis Francisco: "Informática, administración y derecho a la intimidad". En: VARIOS AUTORES: *Introducción a la informática jurídica.* Madrid: Fundesco (Colección: Impactos), 1986 47-61.

[34] 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 Mª: Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información. Madrid: Los Libros de Fundesco (Colección Impactos), 1987. Op cit en la pág. 92].

- Proyecto Ministerial de modificación del Código Penal de Austria (1985) en su Art. 147 (a).
- 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

  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.

Todas estas características se pueden reducir, y esto ocurre en la mayoría de las leyes que hemos visto, a dos aspectos muy concretos que son el reconocimiento del derecho a acceder a la información contenida en un banco de datos y a reivindicar la rectificación, e incluso la eliminación, de todos aquellos datos erróneos o carentes de interés.

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

Tocando a su fin el tema que estamos desarrollando, nos queda por analizar un aspecto importante del mismo como es ¿qué hacemos en España respecto a la protección de datos?.

Vamos a intentar entresacar aquellos puntos de interés que podemos encontrar en nuestra legislación y vamos a acabar el tema especulando un poco acerca de cómo nos gustaría que fuera la Ley española de protección de datos.

V.a. Código Civil

Son muy escasas las normas que nos encontramos en el Código Civil[35], 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"[36], 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 Familiar y a la propia Imagen, que apareció en el B.O.E. Nº 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[37] no sería incorrecto el contemplar la informática como una de las formas de tener

---

[35] Hemos manejado la edición del B.O.E.: *Código Civil*. Madrid: Boletín Oficial del Estado (Serie Universitaria), 2ª ed. de Junio de 1984.

[36] 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*. Madrid: B.O.E. (Serie Universitaria), 1984. Op cit en la pág. 430.

[37] 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. 7º (De las Intromisiones Ilegítimas). En: B.O.E.: *Código de Legislación Informática*. Madrid: Boletín Oficial del Estado, 1988 42-45].

almacenados los datos personales y poder utilizarla para difundir los mismos, por lo que caería dentro de la tutela jurídica de esta ley.

Sin embargo, esta Ley ha dado lugar a que estos tres derechos de la personalidad, es decir: intimidad personal, intimidad familiar y propia imagen, compartan un único bien jurídico protegido que no es otro que la intimidad de las personas, intimidad que se contempla desde dos vertientes diferentes en nuestra Constitución:

- por una parte es un derecho fundamental de las personas, y como tal tiene la máxima protección
- por otro lado es el límite a otros derechos fundamentales también protegidos, como por ejemplo el derecho a la información o la libertad de expresión.

Por ser considerada la intimidad como un derecho fundamental su defensa exige las máximas garantías en su desarrollo como muy bien expresa el Art. 53.2[38] de la Constitución española desarrollado en la Ley de Protección Jurisdiccional de los Derechos Fundamentales de la Persona [Nº62/1978 de 26 de Diciembre], Ley que protege, entre otras, la libertad de expresión, reunión o asociación, la libertad y el secreto de la correspondencia, la inviolabilidad del domicilio, etc. (Art. 1.2)[39].

Otra medida de protección de la intimidad de las personas y de los datos que sobre uno mismo pueden estar almacenados en un banco de datos es una norma muy general del Código Civil encuadrada en el Título XVI, Cap. II, Arts. 1902 a 1910, que podríamos sintetizar en el primero de los artículos que dice:

> *"El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado"*[40].

En realidad es una defensa muy general de cualquier derecho que haya sido violado pero que, al no haber muchas más cosas siempre es una garantía a la hora de denunciar algún caso de intromisión en nuestra inti-

---

[38] Dice así este artículo:

> *"2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios con un procedimiento basado en los principios de preferencia y sumariedad y en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30"*

[Adams: *La Constitución española de 1978*, Madrid: Adams, 1990. Art. 53.2; Cap. IV (De las garantías de las libertades y derechos fundamentales); Sección 2ª (De los derechos y deberes de los ciudadanos); Título I (De los derechos y deberes fundamentales); Op cit en la Pág. 44].

[39] Para más información, se puede consultar esta Ley en: Díaz-Maroto y Villarejo, Julio y Suárez González, Carlos J.: *Código Penal y Legislación Complementaria*. Madrid: Civitas (Biblioteca de Legislación), 16ª ed. actualizada a Septiembre de 1991: Ley de Protección Jurisdiccional de los Derechos Fundamentales de la Persona [Nº62/1978 de 26 de Diciembre] 465-468.

[40] B.O.E.: *Código Civil*. Madrid: Boletín Oficial del Estado (Serie Universitaria), 2ª ed. de Junio de 1984. Op cit en la pág. 371.

midad. Esto mismo podía ser reivindicado desde el Art. 1092 del Código Civil[41].

V.b. Código Penal

En cuanto al Código Penal Español[42] 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[43], 360[44], 367 y 368 que hacen referencia a la revelación de los secretos e informaciones privilegiadas y de su incorrecto uso[45], 497, 498 y 499 que se refieren al descubrimiento y revelación de secretos[46]). No obstante el Proyecto de

---

[41] B.O.E.: *Código Civil*. Madrid: Boletín Oficial del Estado (Serie Universitaria), 2ª ed. de Junio de 1984. Op cit en la pág. 233:

"Las obligaciones civiles que nazcan de los delitos o faltas se regirán por las disposiciones del Código Penal".

[42] Hemos utilizado la edición preparada por Díaz-Maroto y Villarejo, Julio y Suárez González, Carlos J.: *Código Penal y Legislación Complementaria*. Madrid: Civitas (Biblioteca de Legislación), 16ª ed. actualizada a Septiembre de 1991.

[43] 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"

[44] 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"

[45] 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"

[46] 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.

Reforma del Código Penal de 1980 y 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"*[47].

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.

También nos encontramos con otros artículos no relacionados directamente con la protección de la intimidad de las personas pero que tienen una aplicación indirecta, por ejemplo el allanamiento de morada. Si consideramos nuestro hogar como el lugar donde desarrollamos nuestra vida privada, tal y como proponían Samuel D. Warren y Louis D. Brandeis (el hogar de cada uno como nuestro castillo inexpugnable), los artículos 490, 491 y 492 servirán para proteger nuestra intimidad[48].

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"

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

[48] Art. 490:

"El particular que entrare en morada ajena o sin habitar en ella se mantuviere en la misma contra la voluntad de su morador será castigado con arresto mayor y multa de 100.000 a 500.000 pesetas.

Si el hecho se ejecutase con violencia o intimidación, la pena será de prisión menor y multa de 100.000 a 500.000 pesetas"

Art. 491:

"La disposición del artículo anterior no es aplicable al que entra en la morada ajena para evitar un mal grave a sí mismo, a los moradores o a un tercero, ni al que lo hace para prestar algún servicio humanitario o a la justicia"

Art. 492:

"Lo dispuesto en esta capítulo no tiene aplicación respecto de los cafés, tabernas, posadas y demás casas públicas mientras estuvieren abiertas"

En el caso de que el que allanara nuestra vivienda fuera un funcionario público sería suspendido y multado (100.000 a 200.000 pesetas según el Art. 191: "El funcionario público que, no siendo autoridad judicial, entrare en el domicilio de un súbdito español sin su consentimiento, fuera de los casos permitidos por las leyes"[49].

Por último en el articulado comprendido entre el 453 y el 467 nos encontramos todo lo relativo a protección del honor de las personas, la injuria y la calumnia, acciones estas que pueden invadir el espacio interior de cada uno de nosotros. No vamos a tratarlo en este momento ya que no es el punto central de la disertación que estamos llevando a cabo, pero quien esté interesado en profundizar en este tema puede consultar las obras que enumeramos en la siguiente nota a pie de página[50].

Art. 492 bis:

"Salvo los dispuesto en el artículo 491, el que quebrantare la inviolabilidad de un lugar sagrado, edificio religioso u otro inmueble protegido por dicho privilegio por ley especial o convenio internacional, debidamente ratificado, incurrirá en la pena de arresto mayor y multa de 100.000 a 1.000.000 de pesetas.

Si el reo fuera funcionario público o agente de la Autoridad y obrare con abuso de su cargo, se impondrá la pena de prisión menor y multa de 100.000 a 1.000.000 de pesetas"

[Díaz-Maroto y Villarejo, Julio y Suárez González, Carlos J.: *Código Penal y Legislación Complementaria*. Madrid: Civitas (Biblioteca de Legislación), 16ª ed. actualizada a Septiembre de 1991: Cap. V (Del allanamiento de morada); Título XII (De los delitos contra la libertad y seguridad); Libro II (Delitos y sus penas); 233-234].

[49] Díaz-Maroto y Villarejo, Julio y Suárez González, Carlos J.: *Código Penal y Legislación Complementaria*. Madrid: Civitas (Biblioteca de Legislación), 16ª ed. actualizada a Septiembre de 1991. Op cit en la pág. 136.

Los casos permitidos por las leyes son los comprendidos en los artículos 490, 491 y 492 que acabamos de ver.

Aprovechando esta cita, recordaremos que nos encontramos este artículo 191 en: Sección 2ª (De los delitos cometidos por los funcionarios públicos contra el ejercicio de los derechos de la persona reconocidos por las leyes); Cap. II (De los delitos cometidos con ocasión del ejercicio de los derechos de la persona reconocidos por las leyes); Título II (Delitos contra la seguridad interior del Estado); Libro II (Delitos y sus penas); Arts. 178 a 204 bis a); 128-141.

[50] - Díaz-Maroto y Villarejo, Julio y Suárez González, Carlos J.: *Código Penal y Legislación Complementaria*. Madrid: Civitas (Biblioteca de Legislación), 16ª ed. actualizada a Septiembre de 1991: Arts. 453-467; Título X (De los delitos contra el honor); Libro II (delitos y sus penas) 224-227.

- Sánchez Férriz, Remedios: "Las libertades de expresión y de información y los derechos al honor, a la intimidad y propia imagen. En: VARIOS AUTORES: *Información y libertades públicas en España*. Madrid: Universidad Complutense (Cursos de Verano de El Escorial 1989), 1990 173-194.

- López Guerra, Luis: "Límites a las libertades de expresión e información. Honor e intimidad. En: VARIOS AUTORES: *Información y libertades públicas en España*. Madrid: Universidad Complutense (Cursos de Verano de El Escorial 1989), 1990 195-208.

- Lago, Julián: "La Ley orgánica de protección civil del derecho al honor, intimidad y propia imagen, como límite a la libertad informativa". En: VARIOS AUTORES: *Información y libertades públicas en España*. Madrid: Universidad Complutense (Cursos de Verano de El Escorial 1989), 1990 209-219.

- B.O.E.: "Ley Orgánica 1/1982, de 5 de Mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen" [BOE Nº 115 de 14 de Mayo de 1982]. En: B.O.E.: *Código de legislación informática*. Madrid: Boletín Oficial del Estado, 1988. [42-47].

V.c. Anteproyecto de Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales

Después de lo que acabamos de comentar en los epígrafes anteriores, no nos cabe la menor duda de que una Ley sobre el uso de la Informática se está haciendo necesaria[51].

Hubo un tímido intento de elaboración en la década de los 70, más concretamente en el año 1976[52], por parte de la que era en aquella época Escuela Nacional de Administración Pública. Un grupo de trabajo elaboró un borrador, desde la óptica social de ese decenio, acerca de la utilización de los bancos de datos. La idea fue desechada aunque fuera de nuestro país tuvo bastante aceptación.

Posteriormente, 1983, se inició la elaboración del citado anteproyecto, siendo "presentado en sociedad" en un coloquio celebrado en Madrid entre los días 13 y 15 de Junio de 1984 organizado por el Consejo de Europa y la Secretaría de Estado para la Administración Pública.

El texto originariamente, pues hasta que se convierta en Ley ha podido y puede cambiar substancialmente, se dividía en dos partes: los principios generales acerca de la utilización de datos personales, y la regulación para el ejercicio de los derechos de acceso a la información, rectificación de los datos erróneos y supresión de los datos que se consideren oportunos, incluyendo en ambos apartados una serie de situaciones excepcionales en las que no tendría aplicación la ley tal y como quede redactada.

Este anteproyecto recoge la filosofía jurídica de la legislación europea que ya hemos comentado en otra parte y del Convenio 108 del Comité de Ministros del Consejo de Europa (*Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*).

También hemos comentado en otro apartado que se pretende crear la figura del responsable de datos.

Por lo tanto, ¿sobre qué aspectos debe incidir más esta futura Ley?, o mejor dicho, ¿para qué es necesaria una Ley de protección de datos en España?:

1º para recoger 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

---

[51] En la actualidad hay un anteproyecto de ley informática, Lortad, que tiene que pasar a discutirse en el Parlamento Español (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales publicada en el *Boletín Oficial de las Cortes* el 24 de Julio de 1991)

[52] Heredero, Manuel: "La informática y el uso de la información personal". En: VARIOS AUTORES: *Introducción a la informática jurídica*. Madrid: Fundesco (Colección: Impactos), 1986 33-46.

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

3º para impedir el que llegue a ser realidad la profecía de George Orwell[53], es decir, evitar 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

4º 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"[54] sobre la sociedad

5º para conformar adecuadamente el tipo de información que debe incorporarse a un banco de datos, delimitando perfectamente la frontera entre ficheros de datos sensibles y ficheros de datos no sensibles, llegando a prohibir la creación del primer tipo de los que acabamos de enunciar

6º para evitar la introducción, voluntaria o involuntaria, de datos erróneos sobre las personas, arbitrando las medidas necesarias para la corrección de los mismos, así como las revisiones periódicas de los mismos y la eliminación de todos aquellos datos desfasados, obsoletos o que ya no tengan validez en función de los fines para los que fueron recogidos

7º para proteger real y eficazmente la confidencialidad de las personas cuyos datos están almacenados en un banco de datos, siempre que sea posible

8º para identificar a la persona o institución responsable de los datos almacenados

9º para que no se puedan utilizar los datos recogidos con otros fines a los que se predicaron en el momento inicial y, por supuesto, para conocer qué datos van a formar parte de un banco de datos

10º para seleccionar las personas que vayan a trabajar con datos personales.

---

[53] 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 Ernest, Morris L.: "La Ley y la Computadora"; Cap. 17 de la obra *Control Legal de la Nueva Tecnología*. Buenos Aires: Marymar, 1972; 203-217.

[54] Palabras debidas a Rose y que son citadas por Rubén, Brent D.: "En la era de la información: informa-ción, tecnología y estudio del comportamiento". *Documentación de las Ciencias de la Información* (1990) *Vol. 13* Pág. 63.

Estamos seguros de que al lector de estas líneas se le pueden estar ocurriendo otras razones por las que es necesaria una Ley de protección de datos, pero creemos que estos son los aspectos más importantes que deberían tenerse en cuenta a la hora de confeccionar esa normativa.

También estamos convencidos de que antes de dar este paso, lo primero que habría que hacer es un censo de los bancos de datos personales que ya estén en funcionamiento, tanto públicos como privados, para tener conocimiento de los mismos y poder someter a la legislación que se desarrolle el funcionamiento de los mismos[55].

Hoy ya podemos hablar de una Ley[56] sobre la Protección de los Datos Personales en España, que es de lo que nos vamos a ocupar a continuación.

V.d. Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales

La Ley tiene por finalidad "...hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, (...)"[57]. Para ello se Ley se articula en dos partes bien diferenciadas: una general y otra especial. En la primera de estas dos partes o secciones se tratan los derechos y acciones encaminadas a que se cumplan los preceptos generales marcados por la Ley (pautas para la recogida de los datos, como preservar la veracidad de la información, racionalidad en el uso de datos personales, etc.), mientras que la segunda parte es más específica sobre el tema que estamos tratando.

Introduce como novedad lo que denominan el principio de consentimiento, del que hablaremos más adelante pero que viene a significar que para poder introducir nuestros datos personales en cualquier sistema de almacenaje electrónico tienen que informarnos convenientemente y pedirnos permiso.

La Ley se divide en siete títulos[58], 48 artículos, 3 disposiciones adicio-

---

[55] Algo similar se ha hecho en Francia y en el Reino Unido, tal y como nos comenta HEREDERO, Manuel: "La informática y el uso de la información personal". En: VARIOS AUTORES: *Introducción a la informática jurídica*. Madrid: Fundesco (Colección: Impactos), 1986 Op cit en la pág. 46.

[56] Este epígrafe ha sido redactado en dos partes. La primera, justo hasta este punto, que lo redacté antes de que saliese promulgada la Ley de Protección de Datos. La segunda parte, que iniciamos en este momento, se hace teniendo ya promulgada la Ley que puede ser consultada en el B.O.E: Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Boletín Oficial del Estado Año CCCXXXII* (1992) *Nº 262* 37.037-37.045. Por este motivo, en la primera parte utilicemos como forma verbal para construir las frases el futuro y, de ahora en adelante utilizaremos el presente. Se mantienen las dos partes del texto porque creo que resulta interesante ver que opinábamos antes de promulgarse la Ley y que decimos ahora.

[57] B.O.E: Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Boletín Oficial del Estado Año CCCXXXII (1992) Nº 262*. Op cit en la pág. 37.037.

[58] Que vamos a enumerar solamente:

- Título I: Disposiciones generales

nales, 1 disposición transitoria única, 1 disposición derogatoria y 4 disposiciones finales.

Del Título I cabe destacar el ámbito de aplicación de la Ley que se refiere a todos los ficheros que contengan datos de carácter personal:

> *"La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado"*[59].

Se establecen también los casos en los que no se aplicará esta Ley, como por ejemplo los ficheros públicos de publicidad, ficheros personales para uso personal, ficheros que contengan información ya publicada oficialmente, ficheros de temática jurídica a los que puede acceder cualquiera, ficheros de asociados a partidos políticos, sindicatos, etc.

También se establecen los ficheros que requieren alguna disposición específica: ficheros regulados por la legislación de régimen electoral, ficheros sometidos a normativas especiales, ficheros del Registro Civil, ficheros para tareas estadísticas, ficheros sometidos a la Ley Reguladora del Régimen del Personal Militar Profesional.

Como vemos no son muchas las excepciones pero suficientes para que la protección de la intimidad de las personas no quede completada al 100%, aunque podemos quedarnos tranquilos como iremos viendo a lo largo de estas páginas.

Acaba el Título I con unas definiciones que por su interés vamos a transcribir literalmente, al menos las más importantes:

> *"a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.*
>
> *b) Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*
>
> *c) Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de modificaciones, consultas, interconexiones y transferencias.*

- Título II: Principios de la protección de datos
- Título III: Derechos de las personas
- Título IV: Disposiciones sectoriales
  - Capítulo I: Ficheros de titularidad pública
  - Capítulo II:Ficheros de titularidad privada
- Título V:Movimiento internacional de datos
- Título VI:Agencia de protección de datos
- Título VII:Infracciones y sanciones.

[59] B.O.E: Ley Orgánica ... Ibídem. Op cit en la pág. 37.039. Título I Art. 2.1

d) Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo"[60].

En el Título II son muchas cosas las importantes que podemos leer sobre la calidad de los datos, el derecho de información en la recogida de datos, etc., pero los más importantes son sin duda el del consentimiento de las personas a que sus datos estén en un fichero automatizado salvo si los datos se obtienen de fuentes accesibles al público, fuentes laborales, etc. Este consentimiento informado puede no obstante ser revocado. A pesar de este consentimiento hay datos que están especialmente protegidos por la Ley y que no se deben dar si no se quiere: datos sobre la ideología política, religión, creencias, origen racial, salud o vida sexual. En caso contrario hay que dar el consentimiento por escrito. Sea como sea el apartado 4º del Art. 8 deja las cosas bien claras: "Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelan la ideología, religión, creencias, origen racial y vida sexual"[61].

Otros aspectos importantes de este Título II hacen referencia a la seguridad de los datos (establecimiento de las medidas físicas y lógicas para proteger los ficheros de datos personales automatizados: Art. 9), el secreto profesional que deben guardar las personas que trabajan con este tipo de ficheros (Art. 10) o la cesión de los datos (Art. 11).

En el Título III se encuentran los artículos que más nos afectan a las personas pues son los que hacen referencia nuestros derechos, el más importante el 13:

"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero. El Registro General será de consulta pública y gratuita"[62].

Este derecho se complementa con la normativa registrada en el Art. 14 que hace referencia al derecho de acceso de los usuarios a los ficheros que contengan sus datos, o el del Art. 15 que nos da derecho a rectificar o cancelar los datos que consideremos oportunos, recogiéndose también el derecho a las indemnizaciones (Art. 17) en el caso de que se incumpla la normativa.

El Título IV que hace referencia a los ficheros públicos y privados, tienen la misma estructura más o menos, hablando de la creación, modificación o supresión de estos ficheros, la cesión de los mismos y sobre ficheros especiales, por ejemplo los de los Cuerpos de Seguridad del Estado.

---

[60] B.O.E: Ley Orgánica ... Ibídem. Op cit en la pág. 37.039. Título I Art. 3

[61] B.O.E: Ley Orgánica ... Ibídem. Op cit en la pág. 37.040. Título II Art. 7.4

[62] B.O.E: Ley Orgánica ... Ibídem. Op cit en la pág. 37.040. Título III Art. 13

El Título V, sobre el movimiento internacional de los datos, lo que en otro lugar hemos llamado flujo transfronterizo de datos, establece que "No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, (...)"[63], y acaba con las excepciones que no vamos a comentar por no alargar excesivamente este trabajo.

El siguiente Título, el VI, habla de la Agencia de Protección de Datos que será regulada por un estatuto propio aunque sus funciones son velar por el cumplimiento de esta Ley, autorizar la creación de los ficheros, atender a las demandas de los usuarios, informar de los derechos, etc. Contará la Agencia con un Director, un Consejo Consultivo[64] un patrimonio y unos presupuestos.

Para terminar, el Título VII hace referencia a las infracciones, tipificadas en tres grados: leves, graves y muy graves, recogidas en el Art. 43[65], que van desde no tener los datos actualizados, recoger datos sin tener el consentimiento informado de las personas, hasta no guardar el secreto o recoger datos de forma fraudulenta o engañosa. Las sanciones esta vez sí son elevadas, pues una falta leve será sancionada desde 100.000 a 10.000.000 de pesetas, una grave de 10.000.001 a 50.000.000 y una muy grave de 50.000.001 a 100.000.000.

Ni mucho menos acaba aquí una Ley tan importante como la que se acaba de promulgar en nuestro país, pero podemos decir que aquellos aspectos sobre los que debía incidir más esta Ley, tal y como vimos en el apartado anterior, se cumplen sobradamente, por lo que podemos decir que nos encontramos ante una buena Ley cuya efectividad será posible si todos aunamos esfuerzos para que esto sea real. Sólo el tiempo podrá darnos la razón.

---

[63] B.O.E: Ley Orgánica ... Ibídem. Op cit en la pág. 37.042. Título V Art. 32

[64] El Consejo Consultivo estará formado por un Diputado, un Senador, un representante de la Administración Pública y otro de la Local, un miembro de la Real Academia de Historia, un experto del Consejo de Universidades, un representante de los consumidores, otro de las Comunidades Autónomas y un representante del sector de ficheros privados.

[65] Como son muy amplias las sanciones no vamos a transcribirlas. Si alguien está interesado en analizarlas podrá hacerlo en B.O.E: Ley Orgánica ... Ibídem. Op cit en las págs. 37.043/4. Título VII Art. 43.