

PROTECCIÓN DE DATOS. ANÁLISIS COMPARADO DE LA LA LEGISLACIÓN DE ALGUNOS PAÍSES EUROPEOS: ALEMANIA, ESPAÑA, FRANCIA Y GRAN BRETAÑA

FRANCISCO EUGENIO Y LUIS EUGENIO OLIVER

SUMARIO: 1. *Introducción.*—2. *Personalidad.*—3. *Intimidad.*—4. *Datos.*—5. *Legislación.*—6. *Definiciones.*—7. *Principios.*—8. *Infracciones.*—9. *Conclusiones.*

1. INTRODUCCIÓN

Más que con la verdadera realidad de los seres humanos, solemos relacionarnos con la realidad «virtual» (como hoy se dice) de sus datos: la información, la configuración (por vía de expresiones lingüísticas fundamentalmente) de realidades exteriores nos invade sin cesar; el *sujeto representado, atrapado, en la información*, la persona «objetuáda» (valga la expresión) en sus datos (convertida en objeto informativo) está sujeta al riesgo de que sus signos de identidad personales, nominativos, identificadores, biográficos (reales o no, eso no hace al caso: los datos que de ella se nos ofrecen), no sean precisamente fidedignos, dignos o respetuosos con su persona. *Proteger los datos*, la recogida y comunicación de los datos nominativos *de una persona es proteger a la persona misma.*

Para contribuir a una reflexión sobre la materia, hemos optado por presentar algunas consideraciones sobre el tema en el ámbito de la *legislación comparada*. Trataremos de ver lo que se ha hecho, y a partir de ahí quizá se pueda apuntar lo que aún se pueda hacer en orden a una eficaz protección de datos.

Ha sido constante nuestra preocupación por pulir y homologar, en lo posible, los nuevos términos técnicos, surgidos en el ámbito de la informática y de la informática relacionada con el derecho. Esa es una de las conclusiones, nos permitimos anticipar, más evidentes del trabajo: la necesidad de limpiar de

barbarismos la jerga iusinformática, y de fijar en significantes precisos y de amplio poder de comunicación los nuevos conceptos de una ciencia que está, sea dicho con toda propiedad, justamente en sus *balbucesos*.

2. DERECHOS FUNDAMENTALES DE LA PERSONA

Ferrara, el insigne jurista italiano dejó escrito que:

«los derechos de la personalidad son los derechos supremos del hombre, los que le garantizan el goce de sus bienes personales; frente a los bienes externos [puntualizó] los derechos de la personalidad nos garantizan el goce de nosotros mismos, *el señorío sobre la [propia] persona*, la actuación de las propias fuerzas físicas o espirituales».

Las ideas suyas en este párrafo son las ideas de libertad, independencia, autodesarrollo, logro personal.

Entendemos que el derecho a la dignidad, el derecho a la libertad o a la fraternidad no son propiamente derechos subjetivos mientras no se establezcan deberes exigibles del tipo de: deber de respeto a la dignidad de los demás, deber de respeto a la libertad o a la fraternidad. Pero esos deberes no son fáciles de establecer y de exigir. Hay que concretarlos en deberes del tipo de: deber de no violar el domicilio ajeno; deber de no omitir socorro a quien lo necesite; deber de no difundir, o de no almacenar, datos nominativos sin el consentimiento del interesado, etc.

La imparable evolución de la humanidad ha traído consigo transformaciones económicas, sociales, políticas, jurídicas (todo en uno, inseparablemente, o consecuentemente si se prefiere) que han cristalizado en el reconocimiento de derechos de la persona de diferente naturaleza. En un intento de hacer una síntesis de la sucesiva aparición de distintas categorías de derechos de la persona, esto es, de derechos inherentes a la mera condición de ser persona, proponemos el siguiente esquema/resumen:

ÉPOCA/SOCIEDAD/ESTADO	DERECHOS: TIPO/CONTENIDO
1) Revol. burg. francesa/soc. agr./E. Lib	políticos: «libertad»
2) Revol. industrial/soc. ind./E. Social	sociales: «asistencia social»
3) Revol. informática/soc. inf./E. Cultural	informativos: «identidad cultural»

El derecho a la identidad se manifiesta, en alguno de sus aspectos, en el derecho a su intimidad. que comprende, en su dimensión más primaria, el derecho a no ser objeto de observación, de información que se capta y consecuentemente se difunde.

3. DERECHO A LA INTIMIDAD

El derecho a la intimidad lo podríamos definir, para entendernos, como el derecho a impedir la difusión de alguna información sobre nosotros. El derecho a impedir la difusión de información sobre mi persona (aunque con estos otros se relacione; o haya nacido como derivación de ellos) se diferencia hoy de los siguientes derechos: 1, el derecho a la inviolabilidad de domicilio; 2, el derecho al honor; 3, el derecho a la propiedad intelectual y artística. Los bienes jurídicos (jurídicamente protegidos) más inmediatos, visibles y primeramente reconocidos a la persona puede decirse que han sido estos dos: el bien de su VIDA, y el bien de sus BIENES, de su patrimonio, de las cosas de su propiedad. Y, consecuentemente, las dos típicas y más antiguas infracciones jurídicas han girado, por una parte, en torno a la INTEGRIDAD DE LA PERSONA (comprendiendo los ilícitos contra su integridad física; y los ilícitos contra su integridad moral, esto es, la injuria, el deshonor); y, por otra parte, en torno a la INTEGRIDAD DE SU PATRIMONIO.

El derecho a la intimidad tiene concomitancias, por una parte, con el derecho a la integridad de la PERSONA (por cuanto, aun siendo diferente a él, se conecta con el derecho al honor y/o a la dignidad); y, por otra parte, con el derecho a la integridad del PATRIMONIO (por cuanto, aun siendo diferente a ellos, se conecta con el derecho a la inviolabilidad de domicilio [inicialmente objeto de propiedad privada, después incluso objeto de posesión privada] y con el derecho a la propiedad intelectual sobre las obras en que nuestra intimidad aparece: como es el caso de unas memorias íntimas que no queremos que se difundan].

Entre intimidad y vida privada, en castellano, las diferencias no son, creemos, significativas. Se quiere decir, en uno y en otro caso, manifestaciones del comportamiento, del pensar o aun del sentir de una persona que no pasan al ámbito público, que quedan dentro de un círculo cerrado a la generalidad de los demás. En la lengua italiana «intimitá» alude a familiaridad, relación de confianza; y «riservatezza» quiere decir reserva, discrección. Para que los términos «vida privada» «intimidad» o «reserva» adquieran un significado jurídico hay que anteponerles la expresión «derecho a la protección de la ...» [de la intimidad, de la vida privada, de la información reservada o íntima].

4. DATOS NOMINATIVOS: EL DERECHO A SU INVIOABILIDAD: LEGISLACIÓN COMPARADA

El poder de disposición sobre aquello que incumbe a la vida privada de un sujeto (su opiniones, sus sentimientos, su salud, su patrimonio, el interior de su

vivienda, su conducta «en zapatillas» [por decir lo que hace cuando no se expone al público sino que se manifiesta a los de su confianza]) le corresponde precisamente al sujeto en cuestión; y no a un extraño. El derecho a la vida privada, a la intimidad, que viene a ser lo mismo, nació, por obra del artículo de Warren & [and] Brandeis, como una derivación del derecho de *propiedad* relacionado con el deber de *discreción*.

Una persona contrataba los servicios de profesionales (un sirviente doméstico, un abogado, un médico) que, para desempeñar su función, necesitaban entrar en el ámbito de la vida (y, con ello, del patrimonio, de la salud, de los sentimientos, de las costumbres, etc.) de la persona a quienes se prestaba tales servicios. Esta persona que había tenido acceso al conocimiento de la vida privada de una persona [porque entraba físicamente en el ámbito de la vida del otro] debía comportarse con lealtad respecto al sujeto cuya vida privada, en algunos de sus aspectos, conocía. Porque la vida privada era *propiedad* [«privacy-property»] del interesado y de ninguna manera pertenecía al extraño ocasional conocedor de la misma, que estaba obligado, desde luego, a un comportamiento leal, a una *discreción*, con respecto al sujeto protagonista de tal vida privada.

Sin embargo cabe conectar el derecho a la protección de la intimidad, el derecho a la inviolabilidad de la vida privada, con el derecho a la libertad; cabe concebir el derecho a la intimidad como una manifestación del derecho a la libertad. Así lo entendieron Warren y Brandeis.

Desde el momento en que adquiere especial significación la difusión de información sobre la vida de una persona (a partir de, por una parte, el auge de la prensa [el hecho técnico de la aparición de los medios de difusión de la información]; y a partir, por otra parte, de la utilización de las técnicas de la informática y de la telemática) la intimidad puede ser violada mediante la recogida y difusión de dicha información. Porque vulnerando la intimidad de datos personales se viola la intimidad de la persona a la que los datos, de manera muy patente, representan.

5. LEGISLACIÓN

5.1. *Alemania (República Federal de Alemania).*

Ley Federal, de 27 de enero de 1977, para la protección contra el abuso de datos sobre las personas con motivo del tratamiento electrónico de datos. Publicada en el «Boletín de Legislación Federal» (Bundesgesetzblatt), Parte I, número 7, de 1 de febrero de 1977, págs. 201 y sigs. Entrada en vigor: 1 de

enero de 1978 (art. 47); salvo algunos artículos: para el art. 6, sobre medidas técnicas organizativas, la entrada en vigor establecida era la fecha 1 de enero de 1979. La ley alemana de protección de datos consta de 47 artículos más un anejo al Apartado 1 del artículo 6º sobre distintas medidas de control para el cumplimiento de lo dispuesto en la Ley. Se distribuyen los artículos de la Ley en las siguientes seis secciones:

1. SECCIÓN PRIMERA: DISPOSICIONES GENERALES. Se incluye en ella un artículo (el art. 2) dedicado a *Definiciones*.

2. SECCIÓN SEGUNDA: DEL TRATAMIENTO DE DATOS DE LAS AUTORIDADES Y OTROS ENTE PÚBLICOS. Esta Sección está dedicada [como se dice en el art. 7] a los tratamientos de datos cuando la entidad almacenadora de los mismos sea un ente público: una autoridad u otro ente público del *Estado Federal* de corporaciones federales autónomas, instituciones y fundaciones de Derecho público [etc.]; o una autoridad u otro ente público de los *Estados regionales*, municipios y federaciones de municipios [etc.]. Se recoge y regula en esta Segunda Sección de la Ley Alemana la figura del *Comisario Federal para la Protección de Datos*.

3. SECCIÓN TERCERA: DEL TRATAMIENTO DE DATOS DE ENTE NO PÚBLICOS PARA FINES PROPIOS.

4. SECCIÓN CUARTA: DEL TRATAMIENTO COMERCIAL DE DATOS DE ENTIDADES PRIVADAS «NO PÚBLICAS» CON DESTINO EXTERNO.

5. SECCIÓN QUINTA: DE LAS SANCIONES PENALES Y PECUNIARIAS.

6. SECCIÓN SEXTA: DISPOSICIONES TRANSITORIAS Y FINALES.

ANEJO AL APARTADO 1 DEL ARTICULO 6º. De gran alcance práctico. Está dedicado a las medidas de control (de acceso, de transmisión, de organización, etc.) que se habrán de adoptar para la protección de datos.

5.2. España

La Ley Orgánica de Regulación del Tratamiento de Datos es una pieza legislativa largamente gestada y esperada hace tiempo. Es una Ley de fecha 29 de octubre de 1992 (publicada en el Boletín Oficial del Estado del 31 de octubre de 1992). La Lortad (como abreviadamente se la llama) se estructura en: a) una Exposición de motivos; b) el Texto articulado; y c) una serie de Disposiciones complementarias (disposiciones adicionales, disposición derogatoria, disposiciones finales y disposición transitoria).

La exposición de motivos comprende un total de ocho apartados que, teniendo en cuenta los temas de que se trata en cada uno de ellos, podemos titular del modo que sigue: Apartado I (*Una nueva frontera*). Apartado II (*datos personales privados y datos públicos*). Apartado III (*autodeterminación informática*). 4 Apartado IV (*Control público*). 5 Apartado V (*Agencia de control*). 6 Apartado VI (*Normas de autorregulación*). 7 Apartado VII (*Responsabilidad administrativa, no penal*). 8 Apartado VIII (*Al servicio de los derechos fundamentales*).

El Texto articulado de la Lortad comprende cuarenta y ocho artículos, curiosamente los mismos que los de la correspondiente Ley francesa. Los tres primeros artículos de la Lortad, encuadrados en un Título primero sobre Disposiciones generales, se dedican al Objeto de la Ley, a su Ámbito de aplicación y a Definiciones legales previas. Siguen los artículos del Título segundo, sobre Principios de la Protección de Datos, y del Título tercero, sobre Derechos de las personas. Los artículos del Título cuarto se dedican, en resumidas cuentas, al régimen legal de los ficheros, sean de titularidad pública, sean de titularidad privada. Los artículos del Título quinto están dedicados al Movimiento Internacional de Datos. Los del Título sexto a la Agencia de Protección de Datos. Los artículos del Título séptimo se reservan para regular lo referente a Infracciones y Sanciones.

Las Disposiciones añadidas al texto son: 1 DISPOSICIONES ADICIONALES; 2 DISPOSICIÓN DEROGATORIA; 3 DISPOSICIONES FINALES; 4 DISPOSICIÓN TRANSITORIA.

5.3. *Francia*

El 6 de enero de 1978, el mismo año en que aparece el famoso *Informe Nora/Minc. La informatización de la sociedad*, se aprueba la Ley francesa sobre «La informática, los ficheros y las libertades». El texto de la Ley Francesa de protección de datos de 1978 se basa en el proyecto Lecaunet, así llamado por alusión a quien era Ministro de Justicia del Gobierno de Chirac en el momento en que el proyecto se presentó a la Asamblea Nacional para su aprobación. Tal proyecto se elaboró sobre el correspondiente informe que los miembros de la Comisión Informática y Libertades (CIL) presentaron en 1975. La Comisión Informática y Libertades había sido creada por el Presidente de la República en 1974. Consta esta Ley Francesa de protección de datos, de 1976, de 48 artículos repartidos en 7 capítulos. A saber:

CAPÍTULO I: PRINCIPIOS Y DEFINICIONES.

CAPÍTULO II: LA COMISIÓN NACIONAL DE LA INFORMÁTICA Y LAS LIBERTADES. Es misión de esta Comisión «velar por el respeto de las

disposiciones de la presente Ley» (art. 6). Lo que en otras legislaciones es el Director de la Agencia de Protección de Datos (en España), o el Comisario Federal para la Protección de datos y, en su caso, el Inspector del Estado Regional competente (en Alemania), o el Registrador para la Protección de Datos (en Gran Bretaña), eso es aquí (en Francia), *mutatis mutandi*, la Comisión Nacional de la Informática y de las Libertades: un *órgano de control* del uso abusivo de la Informática; del uso en detrimento de los derechos de la persona.

CAPÍTULO III: FORMALIDADES PREVIAS A LA PUESTA EN MARCHA DE TRATAMIENTOS AUTOMATIZADOS.

CAPÍTULO IV: RECOGIDA, REGISTRO Y CONSERVACIÓN DE LAS INFORMACIONES NOMINATIVAS.

CAPÍTULO V: EJERCICIO DEL DERECHO DE ACCESO.

CAPÍTULO VI: DISPOSICIONES PENALES. Para que una ley sea operativa debe sancionar, coaccionar a quien la toque.

CAPÍTULO VII: DISPOSICIONES DIVERSAS. Sobre ámbito de aplicación; calendario, etc.

5.4. Gran Bretaña

Ley de Protección de Datos, de 12 de julio de 1984, por la que se regula el uso de la información tratada automáticamente en relación con personas individuales y la prestación de servicios en relación con dicha información.

Estructurada en Cinco Partes (a la que siguen una serie de Anejos, cuatro en total) la Ley Británica comprende 43 artículos.

1. PARTE I: Disposiciones preliminares. Consta de tres artículos referidos respectivamente a: (art. 1) Definición de datos y expresiones conexas; (art. 2) De los principios de la protección de datos; (art. 3) Del *Registrador* [para la Protección de Datos] y del Tribunal [con competencias en los procesos sobre protección de datos]. El Registrador [que puede ser parangonado al Director de la Agencia de Protección de Datos de la Ley Española] «será designado por Su Magestad mediante concesión de privilegio» [by Letters Patent].

2. PARTE II: Del Registro y la supervisión de los usuarios [de los almacenistas o poseedores o depositarios] de datos [ciertamente ajenos] y de los centros informáticos. Al comienzo de esta Parte II (art. 4) se recogen los pormenores que deben hacerse constar en el documento de inscripción en el Registro

que están obligados a formalizar, para quedar legítimamente constituídos, tanto los poseedores de datos como los explotadores de centros de proceso de datos personales. Después se regulan cuestiones que, dentro del tema *Del Registro*, van desde la «Prohibición de la posesión no registrada de Datos personales» hasta la posibilidad de «Inspección de datos registrados». De los recursos [ante el Tribunal creado por esta Ley de datos, se entiende] es el tema dos artículos que siguen. Se completan las disposiciones precedentes con un grupo de *Disposiciones diversas y adicionales*.

3. PARTE III: Derechos de los titulares de datos. Se recogen aquí el (art. 21) derecho de *acceso*.

4. PARTE IV: De las exenciones. Quiere decirse de los datos que están exentos de tener que someterse a lo que la Ley dispone en sus dos partes anteriores: la Parte III y la Parte II.

6. DEFINICIONES LEGALES

6.1. *Ley Alemana*

La ley alemana se llama, este es su título abreviado, Ley Federal de Protección de Datos. Veamos algunas de sus definiciones:

1) DATOS. [El subrayado es nuestro]. A los efectos de la presente Ley se entiende por DATOS de índole personal los datos *individuales* sobre *circunstancias* personales u objetivas de una *persona física* determinada o determinable (en lo sucesivo, el INTERESADO [art. 2.1]).

2) INTERESADO. Nos remitimos a lo dicho en la definición de datos: persona física determinada o determinable.

3) FICHERO de datos. Una colección de datos, de estructura uniforme que se pueda obtener y *ordenar* conforme a ciertos rasgos y cambiar de ordenación y *evaluar* conforme a otros rasgos determinados, con independencia del procedimiento empleado para ello, si bien no se incluyen en este concepto los documentos sueltos ni colecciones de documentos, a menos que se puedan ordenar y valorar mediante procedimientos automatizados [art. 2.3].

4) TRATAMIENTO de datos. Comprende: [art. 1. art. 2.2]

1. Almacenar [obtención, toma o custodia de datos en un soporte de datos para utilización posterior].

2. Transmitir [dar a conocer...]
3. Modificar [el contenido...]
4. Destruir [hacerlos irreconocibles...]

5) ENTIDAD almacenadora de datos. Toda persona (sea física o jurídica; sea pública o privada) que almacene datos para ella misma o los haga almacenar por otros. Art. 3.1, en relación con art. 1.2.

Los conceptos que en esta y en otras leyes se definen vienen a ser estos: 1) datos; 2) interesado [concernido, afectado, titular del dato, y que se podría decir también de este otro modo: «nominado»]; 3) fichero de datos; 4) tratamiento de datos; 5) titular del fichero.

6.2. Ley Española

1: DATOS. «Datos de carácter personal: Cualquier *información* concerniente a *personas físicas* identificadas o identificables» [art. 3.a]. Podemos decir que se entiende por dato nominativo informatizado (DNI) cualquier INFORMACIÓN que sea: [a] PERSONAL, es decir, referida a una persona; [b] AUTOMATIZADA, es decir, registrada, elaborada o difundida por medios automáticos, mediante ordenador; y [c] NOMBRADORA de la persona a la que refiere. Los datos que aquí nos interesan no son los exclusivamente numéricos sino la información de cualquier tipo referida a una persona, con tal de que, por consecuencia de estar mediatizada por la acción de la computadora, del ordenador, esté digitalizada, convertida en señales digitales binarias, ceros y unos, que son aquellas con las que los ordenadores trabajan, que los ordenadores «entienden».

2: INTERESADO, afectado, titular, concernido. «*Afectado*: persona física *titular* de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo» [art. 3.e].

3: FICHERO. «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» [art. 3.b].

4: TRATAMIENTO. «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 *comunicaciones*, consultas, interconexiones y transferencias [art. 3.c].

5: TITULAR del fichero. «Responsable del fichero: Persona física, jurídica [sic] de naturaleza pública o privada y órgano administrativo que *decida* sobre la finalidad, contenido y uso del tratamiento» [art. 3.d]. La Ley Alemana es más correcta sintacticamente, al tiempo que más simple y muy eficaz. Dice la Ley Alemana: toda persona (sea física o jurídica; sea pública o privada) que [o bien] *almacena* datos [o bien] los haga *almacenar* por otros [Ley Alemana, art. 3.1].

6.3. Ley Francesa

1) DATOS. «A efectos de la presente ley, se consideran *nominativas* las *informaciones* que permiten, bajo cualquier forma, directamente o no, la identificación de las personas físicas a las que estas informaciones se refieren, con independencia de que el *tratamiento* se efectúe por una persona física o jurídica» [art. 4].

2) INTERESADO. Se emplea esta expresión «el interesado» [«l'interessé»] cuando se dice que «Está prohibido introducir o conservar en memoria informatizada, salvo acuerdo expreso del *interesado*, los datos nominativos [«des données nominatives»]...» etc. [art. 31]. En alguna ocasión se habla (art. 26) de «informaciones nominativas que le conciernen» [de ahí derivaría *concernido*].

3) FICHERO de datos. La Ley francesa no define expresamente qué se entiende por fichero de datos nominativos. En ocasiones, con innegable acierto, utiliza el sugerente sinónimo de *memoria informatizada* [art. 31: «Está prohibido introducir o conservar en memoria informatizada ...»]

4) TRATAMIENTO de datos. «La Comisión [la Comisión Nacional de la Informática y las libertades, que es el órgano encargado de controlar las aplicaciones de la informática a los *tratamientos informativos*, como en el art. 6 se dice] vela por que los *tratamientos automatizados*, públicos o privados, se efectúen conforme a las disposiciones de la presente ley», dice el art. 14.

5) ENTIDAD. La Ley francesa habla de *tratamientos automatizados* [de información] llevados a cabo por cuenta de: el Estado; un organismo público o colectividad territorial, una persona jurídica de derecho privado gerente de un servicio público [art. 15]; y de los *tratamientos* llevados a cabo por personas distintas a las anteriores [art. 16], cabe decir, de *tratamientos* correspondientes a ficheros de *titularidad* privada.

En algún lugar se habla [art. 19] de la persona que tiene capacidad de *decidir* la creación del tratamiento.

6.4. Ley Inglesa

1) DATOS. [El subrayado es nuestro]. Art. 1.1:

«Se entiende por «datos» la *información grabada* en una forma tal que pueda ser tratada por *aparatos que funcionen automáticamente* en respuesta a instrucciones emitidas con este fin».

Art. 1.2:

«Se entiende por «datos personales» datos consistentes en información referente a una *persona viva que sea identificable* con esa información [...]».

2) INTERESADO. Aparte de lo que se dice la definición de datos, la ley define qué debe entenderse por «titular de los datos [Data subject]». Art. 1.4:

«Se entiende por titular de los datos (Data subject) a toda persona individual que fuere el *sujeto de datos* de tipo personal» [nominativos, cabría decir].

3) FICHERO de datos. No recoge expresamente la Ley este término entre los que define (curiosa paradoja, se omite un término, «File», que se ha impuesto como anglicismo aceptado en la generalidad de los idiomas para designar lo que es precisamente un «Fichero» o Archivo). Dice así esta Ley, art. 5.a (a propósito de la definición del poseedor de datos):

«los datos forman parte de una *colección de datos* tratados, o destinados a serlo»

por el poseedor de datos o por el explotador de datos en un centro informático a su cargo.

4) TRATAMIENTO de datos. Art. 1.7:

«Se entiende por tratamiento, en relación con cualesquiera datos, toda modificación, ampliación, supresión, o *reordenación* de los mismos, así como toda *obtención* de la información constitutiva de los mismos, y, en el cada de datos de tipo personal, la realización de cualquiera de estas operaciones con referencia al titular de los datos».

5) ENTIDAD almacenadora de datos. La Ley Inglesa habla de dos tipos de sujetos titulares, por así decirlo, de los ficheros que contienen datos elaborados por procedimientos automatizados.

Estos dos tipos de sujetos son, dicho con palabras que no están en la ley pero que reflejan el sentido de la misma (art. 4.1), los siguientes: A) quien dispone de los datos; B) quien dispone de un centro de tratamiento de datos.

7. PRINCIPIOS

7.1. Alemania

No hay en la Ley Alemana un apartado que expresamente proclame los principios que rigen, en defensa del titular de los datos, el tratamiento automatizado de los mismos. Pero no resulta difícil, rastreando en su articulado, encontrar elocuentes muestras de cada uno de los cinco principios que consideramos fundamentales. Así:

1. Disponibilidad privada y derecho de acceso y rectificación. Art. 3:

«El tratamiento de datos de índole personal protegidos por la presente Ley será lícito [...] únicamente cuando [...] 2) el interesado hubiese dado su *consentimiento*».

Art. 4:

«Todos tendrán derecho, dentro de lo dispuesto en la presente Ley, a / 1) *recibir información* sobre los datos almacenados acerca de los mismos»; / 2) a la *corrección* de los datos almacenados sobre ellos mismos [relativos a su propia persona], cuando fueren inexactos.»

2. Intervención pública. Art. 39:

«Las personas, sociedades y otras asociaciones citadas en el artículo 31 [es decir la que sean de Derecho privado, así como las empresas de Derecho público que actúen en régimen de competencia mercantil] [...] deberán *notificar el comienzo de su actividad* al Supervisor [regional] competente «*der zuständigen Aufsichtsbehörde*» dentro del plazo de un mes».

3. Seguridad de los ficheros. Art.6:

«1. Quien efectuar [...] tratamiento de datos de índole personal deberá adoptar [...] la medidas [de *seguridad*] obligatorias establecidas en el anejo a la presente Ley».

Anejo al art. 6.1:

«Cuando se traten informáticamente datos de índole personal, se adoptarán [...] medidas [...] para: / 1) impedir a personas extrañas el acceso a las instalaciones de tratamiento de los datos [...] (control de acceso); [...]».

4. Confidencialidad. Art 5:

«Se prohíbe [...] todo tratamiento, *revelación*, autorización de acceso a terceras personas [...] sin licencia para ello [...]».

5. Olvido. Art 27:

«2. Podrán ser destruidos datos de índole personal [...]. Deberán ser *destruidos* cuando su almacenamiento fuere ilícito [...]»

7.2. España

Se dice en la Exposición de Motivos (Apartado 2):

«Los principios generales, por su parte, definen las *pautas* a las que debe atenderse la recogida de datos [...]. Este principio, verdaderamente cardinal, de la congruencia y la *racionalidad* [...]».

Demasiada abstracción, pensamos. El texto articulado de la Ley Española dedica el Título II a «Principios de la protección de datos»; de lo que se trata en él es de algunos (así) principios limitativos de la actividad de los titulares de ficheros o elaboradores de datos, de algunos de sus deberes: deber de seguridad, deber de secreto, etc. Entendidos como ideas madre en las que se sustentan los deberes de los elaboradores de datos y, consecuentemente, los derechos de los interesados, los principios de la elaboración de datos hay que buscarlos, camuflados, en la enunciación de tales deberes y de tales derechos.

1. Disponibilidad privada y derecho de acceso y rectificación. Art. 6.1:

«El tratamiento [...] requerirá el *consentimiento* del afectado <sic> [...]».

Art. 14.1:

«El afectado tendrá derecho a solicitar y *obtener información* de sus datos [...] incluidos en los ficheros [...]».

Art. 15.2:

«Los datos [...] que resulten inexactos o incompletos serán *rectificados* y cancelados en su caso.»

2. Intervención pública. Art. 24.1:

«Toda persona o entidad que proceda a la creación de ficheros [...] lo *notificará* previamente a la Agencia de Protección de Datos.»

Además: art. 43.3.a; art. 43.3.i; art. 43.3.j; art. 43.4.f; etc.

3. Seguridad de los ficheros. Art. 9.1:

«El responsable del fichero «en el sentido de el titular, el que tenga los datos bajo su dominio» deberá adoptar las medidas técnicas y organizativas necesarias que garanticen la *seguridad* de los datos [...] y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología [...]».

También art. 43.3.h; y otros.

4. Confidencialidad. Art. 10:

«El responsable [¿director?] del fichero automatizado y quienes intervengan en cualquier fase del tratamiento [...] están obligados al *secreto* profesional [...]»;

Art. 11 (limitación de la *cesión*).

5. Olvido. Art. 4.5 («serán *cancelados*»); Art. 20.4 («se *cancelarán*»).

7.3. Francia

Al comienzo de la Ley Francesa hay como tres proclamas. Una [art. 1]: la informática debe estar al *servicio de todo ciudadano* «principio quizá de beneficencia (?) de los tratamientos». Otra [art. 3]: «ppio. quizá de accesibilidad a los propios datos tratados». Otra [art. 2]: «ppio. quizá de insignificancia jurídica del perfil personal resultante del tratamiento; o de la impugnabilidad de decisiones judiciales, administrativas o privadas fundadas en un perfil electrónico». La «accesibilidad» se puede reconducir a nuestro principio de Disponibilidad privada. Y la «impugnabilidad de decisiones basadas en un perfil electrónico», se encuadra en la limitación de las posibilidades de uso legítimo de los datos, dentro de la Confidencialidad. Sigamos nuestro esquema.

1. Disponibilidad privada y derecho de acceso y rectificación. Art. 25:

«Está prohibida la recogida de datos llevada a cabo por medios fraudulentos, desleales o ilícitos».

Art. 26:

«Toda persona física tiene el *derecho de oponerse* por razones legítimas a que informaciones nominativas que le conciernen sean objeto de tratamiento».

Art. 27:

«Las personas de las que se recojan las informaciones nominativas deben ser informadas: [...] de la existencia de un derecho de *acceso* y de *rectificación*».

2. Intervención pública. Art. 16:

«Los tratamientos automatizados de informaciones nominativas «correspondientes a ficheros de titularidad privada», antes de que sean llevados a cabo, deberán ser objeto de una *declaración* presentada a la Comisión Nacional de la Informática y de las Libertades. / Esta declaración conlleva el compromiso de que el tratamiento se ajusta a lo exigido por la Ley».

3. Seguridad de los ficheros. Art. 19:

«La petición de informe «a la Comisión Nacional» o la declaración «constitutiva de elaborador de datos» ha de precisar las medidas adoptadas para garantizar la *seguridad* de [...]»

4. Confidencialidad. Art. 29: (*No comunicación a terceros*)

5. Olvido. Art. 28: (Los datos no deben ser *conservados* por más tiempo..)

7.4. Gran Bretaña

Lo Ley inglesa (Anejo I, Parte I) dedica 8 párrafos a describir otros tantos principios. Vamos a enunciarlos, buscando expresiones sintetizadoras, del siguiente modo: Uno (1), LEGALIDAD de cualquier actuación respecto a los datos; y en concreto legalidad de los *procedimientos de recogida* de los datos. Dos (2), LEGALIDAD de los *finés de la recogida* (significa que los fines han debido ser declarados). Tres (3), COMPATIBILIDAD entre la utilización declarada de los datos y utilización practicada de los datos. Cuatro (4), PERTINENCIA de los datos recogidos (adecuados, pertinentes y no excesivos), determinada por su finalidad. Cinco (5), VERACIDAD de los datos recogidos. Seis (6), TEMPORALIDAD de los datos, determinada por su finalidad. Siete (7), ACCESIBILIDAD de los datos para el interesado. Ocho (8) SEGURIDAD de los datos, protección física y lógica: adopción de medidas que les hagan invulnerables. Todos estos principios reconocidos como tales por la Ley en los ocho párrafos de referencia, y aun otras ideas básicas repartidas por el texto de la Ley, pueden ser reconducidos a nuestros cinco principios. Veamos.

1. Disponibilidad privada y derecho de acceso y rectificación. La idea de la (1) LEGALIDAD de los procedimientos de recogida de datos (aparte de su conectabilidad con el principio de Intervención pública) implica que éstos no se

pueden obtener sin *consentimiento* del interesado. La idea de (5) VERACIDAD conlleva (además de la de Intervención pública) la idea de que adulterar datos ajenos viene a ser, a los efectos, lo mismo que apoderarse de ellos sin el *consentimiento* de su dueño: porque es el interesado quien tiene el poder de controlarlos, de disponer de la suerte de sus datos. Por último, la idea de (7) ACCESIBILIDAD de los datos para el interesado deriva directamente de la idea de Disponibilidad privada y *derecho de acceso* y rectificación.

2. Intervención. Principio implícito en el de (2) LEGALIDAD de fines *declarados*. Existe, además, un Registro de usuarios [declarados] (art. 4).

3. Seguridad. Es un principio ya indicado: (8) SEGURIDAD.

4. Confidencialidad. Véase (3) COMPATIBILIDAD; y (4) PERTINENCIA. Son límites a la *revelación* de datos. Como los *límites* del art. 5.2.d.

5. Olvido. Es, en esencia, el principio de (6) TEMPORALIDAD.

8. INFRACCIONES (DEBERES, INFRACCIONES Y SANCIONES)

8.1. Alemania

8.1.A INFRACCIONES (A = Administrativas; P = Penales)

1: *Disponibilidad violentada*. Constituye infracción:

1.A) [A]: (1) REGISTRAR, almacenar datos de tipo personal sin informar al interesado (art. 42.1.1):

«Art. 42, Infracciones administrativas, 1. Cometerá infracción administrativa quienquiera que deliberada o negligentemente: 1) no informe al interesado, en contra de lo que dispone el artículo 26, apartado 1 (...).»;

Art. 26.1:

«La primera vez que se almacenen datos referentes a la persona del interesado, *se informará* a éste del hecho, a menos que ya hubiere tenido conocimiento del hecho por otro conducto».

2: *Intervención pública desatendida*. Constituye infracción:

2.A) [A]: (2) NO CUMPLIR el deber de designar por escrito un *encargado de la protección de datos* (art. 42.1.2):

«no designe ningún encargado de la protección de datos [einen Beauftragten für den Datenschutz]»

o no lo designe a tiempo, contra lo dispuesto en los artículos 28, apartado 1, y 38., en relación con el 28, apartado 1: [art. 28.1]:

«Las personas que traten informáticamente datos de índole personal y ocupen en ella un mínimo de 5 trabajadores a título permanente deberán *designar por escrito un encargado* de la protección de datos. La misma norma se aplicará cuando se traten de otra manera datos de índole personal, siempre que por regla general se empleen en ello 20 trabajadores como mínimo de modo permanente».

2.B) [A]: (3) NO CUMPLIR el deber de *notificar a la autoridad competente el comienzo de la actividad del tratamiento* de datos (art. 42.1.4: [no curse como es debido la preceptiva notificación de constitución a que se refiere el artículo 39]; Art. 39.2:

«Con la notificación [del comienzo, cese o modificación de la actividad del tratamiento comercial de datos a la autoridad competente] se comunicarán para el registro de la propia autoridad de tutela los datos siguientes: 1. Nombre o razón social, 2. Titular de la empresa; o Titular de la empresa concesionada / 3.- Dirección postal, 4.- FINES del tratamiento, 5.- Instalaciones: MEDIOS, 6.- Nombre del ENCARGADO, 7.- Tipo de DATOS, 8.- RECEPTOR regular de los datos, si procede».

2.C) [A]: (4) NO PERMITIR la *inspección* necesaria a que se refiere el artículo número 40 de la Ley (art. 42.1.5).

· 3: *Seguridad omitida.. ¿Constituye infracción?*:

De la *seguridad* de los datos a que también el interesado tiene derecho se ocupa, como se ha dicho, el artículo que se refiere a Medidas técnicas y organizativas (art. 6), y el Anejo al Apartado 1 del artículo 6 (con que el texto de la Ley termina). Si la información que conste en la notificación constitutiva de un almacén de datos personales automatizados no constituyera garantía de que los datos a tratar estarán seguros ¿el Supervisor del Estado Regional correspondiente tomará las decisiones pertinente para que el tratamiento de datos no se lleve a cabo?. Debería ser así. La Ley guarda silencio sobre esta infracción.

4: *Confidencialidad quebrada.. Constituye infracción:*

4.A) [A]: (5) TRANSMITIR datos personales *sin cumplir las necesarias formalidades previas* (art. 42.1.3 [«contra lo dispuesto en el apartado 2, inciso segundo del artículo 32, no especifique las RAZONES o los medios de prueba a que dicho precepto se refiere]; Art.32.2 Será lícita la TRANSMISIÓN de datos de índole personal cuando el receptor hubiese acreditado fidedignamente un

interés legítimo en el conocimiento de los mismos. Se deberán especificar en este punto las razones de ese interés legítimo, así como los medios para su demostración fidedigna).

4.B) [P]: (6) TRANSMITIR datos personales *sin estar autorizado* para ello (art. 41.1):

«Quienquiera que sin estar autorizado para ello: 1) transmita o modifique datos personales protegidos por la presente Ley, y que no fueren públicos y notorios; 2) detraiga esos datos o se los procure de ficheros contenidos en recipientes con cierre, será castigado con pena de [...]».

5: *Olvido infringido*. ¿Constituye infracción?

Con respecto al olvido hay un reconocimiento del derecho que tiene el interesado «a que se destruyan los datos almacenados acerca de ellos mismos» cuando se den ciertas circunstancias (art. 4); se deduce que alguien habrá que tenga la obligación de satisfacer este derecho; pero no hemos observado en la Ley disposición alguna que «sancione» especialmente al no cumplidor de ese deber.

8.1.B SANCIONES (A = Administrativas; P = Penales)

A = Sanciones Administrativas

— 50.000 marcos alemanes de multa, máxima sanción

P = Sanciones Penales

- DOS AÑOS de prisión, máxima sanción; o, alternativamente
- multa (alternativamente a la prisión)

Has dos tipos de sanciones en la ley Alemana para el contraventor de la Ley de protección de datos (incluido aquí, como se ve leyendo el art. 41.1, el extraño que «hurta» datos o que los «daña»). Unas son penales (art. 41) y otras administrativas (art. 42).

Art. 42.2. Toda infracción administrativa podrá ser castigada con multa de hasta 50.000 (cincuenta mil) marcos alemanes.

Art. 41.1. [el sancionado con sanción penal /porque «transmita», «modifique» o «detraiga» datos/] «será castigado con pena de prisión de hasta UN AÑO O bien con multa».

Art. 41.2. Si el infractor actuare por el pago de una suma o con intención de lucrarse él mismo o de que se lucre un tercero o de perjudicar a otro, la pena será de prisión hasta dos años o multa.

Art. 41.3. El infractor será perseguido únicamente a instancia de parte.

En lo tocante a la regulación de las infracciones y sanciones, el texto de la Ley Alemana resulta, en comparación con el de la Ley Española, muy escueto en cuanto a los supuestos constitutivos de delitos o de infracciones administrativas, y sin matices, sin graduaciones, en la sanción penal y la sanción económica.

8.2. España

8.2.A INFRACCIONES: (***) muy graves; ** graves; * leves).

1: Disponibilidad violentada. Constituye infracción:

1.A) [***]: (1) RECOGER datos *en forma fraudulenta* [art.: 43.4.a]. (2) (3) (4) Recoger *datos sensibles* (ideológicos y biológicos) [Art.: 43.4.c, con reenvío a: art. 7.2; art. 7.3; y art. 7.4].— 1.B) [**]: (5) Recoger datos sin haber obtenido el *consentimiento* del interesado o sin facilitarle las informaciones previas necesarias. [Art.: 43.3.c; reenvío a art. 5]. (6) (7) No atender al *derecho de acceso, de rectificación y de cancelación* que puede ejercitar el interesado [art.: 43.3.e; art.: 43.3.f].— 1.C) [*]: (8) No atender al *derecho de rectificación y cancelación* (por errores, lagunas o inexactitudes de tipo formal) [art.: 43.2.a)]

2: Intervención pública desatendida. Constituye infracción:

2.A) [***]: (9) Recoger (y, en su caso, elaborar datos *de modo anticonstitucional* (cuando se impida el ejercicio de dchos fundamentales) [art.:43.4.f]. (10) NO CUMPLIR una *orden de suspensión de elaboración* de datos proveniente del Director de la Agencia de Protección de Datos, o del propio interesado [art.: 43.4.d].— 2.B) [**]: (11) Crear un fichero de titularidad pública sin el trámite de la oportuna *autorización* publicada en el B.O.E. o diario oficial correspondiente [art.: 43.3.a]. (12) Crear un fichero de titularidad privada sin el tramite de *notificación* a la Agencia de Protección de Datos (y aun no atender el deber de *proporcionar* a la misma Agencia de Protección de Datos los documentos o informaciones oportunas [art.: 43.3.i]). (13) Crear un fichero de titularidad privada para fines diferentes de los que son los *fines legítimos de la empresa* que crea tales ficheros [art.: 43.3.b]. (14) Elaborar datos, o consiguientemente utilizarlos, de modo *ilícito*, esto es, incumpliendo los *principios y garantías* de protección establecidos, cuando tal hecho no constituya una infracción muy grave

[art.: 43.3.d]. (15) No cumplir los deberes correlativos al derecho de inspección que corresponde a la Agencia de Protección de Datos (APD) [art.: 43.3.j].— 2.C [*]: (16) No cumplir instrucciones o peticiones de la APD [art.: 43.2.b]. (17) No cumplir deberes relativos a cuestiones formales [art.: 43.2.d].

3: *Seguridad omitida*. De los cinco principios: el tercero, adoptar las medidas de seguridad necesarias para garantizar la conservación del depósito de datos y la inaccesibilidad a él por quienes no estén autorizados. Constituye infracción:

3.A) grave [**]: (18) NO CUMPLIR el deber de adoptar las *medidas de seguridad* necesarias para la conservación y custodia de los datos [art.: 43.3.h].

4: *Confidencialidad quebrantada*. De los cinco principios: el cuarto, no quebrar el secreto del dato. Constituye infracción:

4.A) muy grave [***]: (19) DIFUNDIR *datos sensibles* [salud incluida] [art.: 43.4.g (reenvío: arts. 7.2 e 7.3)]. (20) Comunicar, difundir (o ceder) datos nominativos [art.: 43.4.b]. (21) Transmitir (transferir) los datos fuera del ámbito nacional (transferencia *internacional* de datos) cuando el país de destino no tenga legislación equiparable [art.: 43.4.e].

4.B) grave [**]: (22) No cumplir el deber de *mantener el secreto* sobre datos nominativos ajenos (cuando el hecho no constituya una infracción muy grave) [Art.: 43.3.g].

5: *Olvido infringido*. De los cinco principios: el quinto, cancelar cualquier dato prescrito. Constituye infracción:

5.A) leve [*]: (23) No atender al derecho de actualización y conservación de datos sobre los cuales procede la actualización [art.: 43.2.c].

8.2.B SANCIONES

[***] Infracción muy grave. Se sanciona con (a tenor del art. 44.3):

— 100:000.000 pesetas, multa máxima

— 50:000.001 pesetas, multa mínima

[**] Infracción grave. Se sanciona con (a tenor del Art. 44.2):

— 50:000.000 pesetas, multa máxima

— 10:000.001 pesetas, multa mínima

[*] Infracción leve. Se sanciona con (a tenor del Art. 44.1):

— 10:000.000 pesetas, multa máxima

— 100.000 pesetas, multa mínima

A tenor de lo dispuesto en el citado art. 44:

a)

«La cuantía de las sanciones se graduará atendiendo a:

- la naturaleza de los derechos personales afectados,
- al volumen de los tratamientos efectuados,
- a los beneficios obtenidos,
- al grado de intencionalidad y
- a la reincidencia» (art. 44.4)

b)

«El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios» (art. 44.5).

8.3. Francia

8.3.A INFRACCIONES: [**** gravísimas; *** muy graves; ** graves; * leves]

1: Disponibilidad violentada. Constituye infracción:

1.A) [***]: /1/ RECOGER datos mediando fraude (art. 42 en relación con art. 21). /2/ Recoger datos mediando oposición del interesado (art. 42 en relación con art. 26)

2: Intervención pública desatendida. Constituye infracción:

2.A) [**]: /3/ Crear un, digamos, depósito de datos personales sin autorización para ello (art. 41).

2.B) [****]: /4/ Tratar datos de modo abusivo [realizar tratamientos que excedan los límites de lo autorizado] (art. 44).

3: *Seguridad omitida*. Constituye infracción:

3.A) [***] /5/ NO CUMPLIR las oportunas medidas de seguridad, omitirlas (art. 42).

4: *Confidencialidad quebrantada*. Constituye infracción:

4.A) [*] /6/ DIFUNDIR, comunicar datos ocasionando daño a la reputación o a la intimidad del sujeto (art. 43)

5: *Olvido infringido*. Constituye infracción:

5.A) [**] /7/ NO CUMPLIR con el deber de cancelación espontánea de los datos [conservarlos extemporáneamente] (art. 42 en rel. con art. 28).

8. Infracciones (Deberes, Infracciones y Sanciones)

8.3.B SANCIONES

[****] Infracción gravísima. Se sanciona con (a tenor del art. 44):

: 5 años, pena máxima (mínima de un año) y

— 2:000.000 (dos millones) de francos, multa máxima.

[***] Infracción muy grave. Se sanciona con (a tenor del Art. 42):

: 5 años, pena máxima (mínima de 12 meses) y

— 20.000 francos, multa máxima (mínima de 20.000 francos)

[**] Infracción grave. Se sanciona con (a tenor del Art. 41):

: 3 años, pena máxima (mínima de 6 meses) y

— 200.000 francos, multa máxima; (mínima de 2.000).

[*] Infracción leve. Se sanciona con (a tenor del Art. 43):

: 0,5 años (seis meses) pena máxima; (mínima de 2 meses) y

— 20.000 francos, multa máxima; (mínima de 2.000 francos).

Ciertamente, las cantidades de las multas expresadas en francos no son comparables con las cantidades de las multas expresadas en la moneda de otro país.

Por tal motivo será muy práctico y conveniente realizar la oportuna conversión de todas las cantidades tomando una unidad monetaria como referencia.

8.4. Gran Bretaña

8.4.A INFRACCIONES [/: sin determinación de su nivel de gravedad]

1: *Disponibilidad violentada*. Constituye infracción:

1.A [/: [1] RECOGER datos por procedimientos fraudulentos o no legales (Anejo 1. Parte II. Párrafo 1.1):

«A reserva de lo dispuesto en el apartado 2 siguiente, para determinar si una información se ha obtenido lícitamente hay que tener en cuenta el procedimiento por el que fue obtenida, y en particular si la persona de quien se obtuvo fue *engañada o inducida a error* en cuanto a la finalidad o finalidades para las que dicha información haya de guardarse, usarse o revelarse».

2: *Intervención pública desatendida*. Constituye infracción:

2.A [/: [2] NO CUMPLIR el deber de *inscribir* en el Registro el, digamos, depósito de datos (art. 5.5 [en relación con art. 5.1; traslación no literal]: Será reo de delito quien contravenga la prohibición de: a) tener los datos sin haber cumplido la formalidad de presentar una instancia de *inscripción* indicando ciertos pormenores; b) tenerlos y disponer de ellos [mas allá] fuera de los *pormenores* admitidos, que versan sobre: naturaleza de los datos a registrar, fines, fuentes, destino: ámbito personal, destino: ámbito territorial).

2.B [/: [3] No cumplir el deber de *presentar la información* necesaria en el Registro (art. 6.5 [en relación con art. 6.6; traslación no literal]: Será reo de delito quien contravenga el mandato de: a) solicitar la *modificación* de inscripción, cuando proceda; b) suministrar *información clara y verdadera* en las solicitudes de inscripción o de modificación de inscripción).

2.C [/: [4] No atender a un mandamiento judicial de inspección del depósito de datos (art. 16 [De las facultades de entrada y de *inspección*]:

«Será aplicable el Anejo 4 de esta Ley para la averiguación de delitos en el sentido de la presente Ley y en relación con *cualesquiera infracciones a los principios de la protección de datos*».

Anejo 4 [titulado «De las facultades de entrada e inspección»], párrafo 12 [titulado «De los delitos»]; dice así:

«Toda persona que: / a) obstruya intencionadamente a otra en la ejecución de un mandamiento expedido al amparo del presente Anejo, o que / b) sin excusa razonable no facilite al ejecutor del mandamiento toda ayuda que éste le exija razonablemente para la ejecución, / incurrirá en *responsabilidad criminal*».

3: *Seguridad omitida*. Constituye infracción:

3.A [/]: [5] No atender un requerimiento del Registrador sobre medidas de seguridad de los datos (art. 10 [traslación no literal]: Será reo de delito quien contravenga un requerimiento [una orden] del Registrador por el que se le inste a adoptar las medidas de protección de datos que se le indiquen).

4: *Confidencialidad quebrada*. Constituye infracción:

4.A [/]: [6] DIFUNDIR datos que no puedan ser revelados (art. 15.1):

«Ningun dato personal en relación con el cual se estén prestado servicios por una persona que explote un centro informático podrá ser *revelado* por esa persona sin previa autorización de la persona para quien se presten esos servicios [mandatario]».

Art 15.2:

«Será también aplicable el apartado 1 anterior a todo servicio o *agente de la persona* que esté explotando el centro informático».

Art. 15.3:

«Será reo de *delito* toda persona que deliberada o negligentemente infringere el presente artículo»).

4.B [/]: [7] Transferir fuera del ámbito nacional datos que no puedan ser transferidos (art. 12.10 [traslación no literal]: Será reo de delito quien infringiere un aviso [del Registrador] de prohibición de transferencia).

5: *Olvido infringido*. Constituye infracción:

5.A [/]: [8] No cumplir el deber de cancelar de oficio los datos prescritos. (Anejo 1. Parte I. Párrafo 6 [establece el principio de TEMPORALIDAD de los datos]). Como ya se ha indicado, el Anejo 1 se ocupa «De los principios de protección de datos». Consta este anejo de dos partes: Parte I, De los principios; y Parte II, Interpretación [dedicada a la interpretación legal de los principios]. En la Parte I, hay un Párrafo 6; dice así:

«Los datos personales, sea cual fuere su finalidad o finalidades, no se guardarán más *tiempo* del necesario para dicha finalidad o finalidades».

De este párrafo no hay interpretación legal.

8.4.B SANCIONES (a tenor del art. 19)

[a] Infracción de *resistencia a mandamiento judicial* (art. 16 / Anejo 4.12)

TRAMITE: procedimiento sumario

— multa de quinto nivel, máxima [LEC art. 75] (art. 19.3)

[b] Infracción de otro tipo con TRAMITE: procedimiento sumario

— multa no superior al máximo legal [LEC art. 74] (art. 19.2.b)

[c] Infracción de otro tipo con TRAMITE: juicio contradictorio

— multa (art. 19.2.a).

Notas complementarias

1. LEC significa Ley de Enjuiciamiento Criminal de 1982

2. Hay ciertos supuestos de delitos en los que el Tribunal por el cual o ante el cual fuere condenada una persona puede ordenar que se *confisque*, se *destruya* o se *borre* cualquier dato sustantivo que en opinión de tal Tribunal guarde relación con el hecho de la comisión del delito. Estas delitos (a tenor del art. 19.4) son los siguientes:

1) poseer un depósito de datos personales sin haber realizado la correspondiente *inscripción* en el Registro (art. 5).

2) incumplir un *requerimiento del Registrador* para la Protección de Datos pidiendo al titular del depósito de datos que se ajuste en su conducta a los principios de protección de datos de cuyo incumplimiento el Registrador tiene certeza (art. 10).

3) realizar, contraviniendo una prohibición expresa del Registrador, *transferencias* de datos fuera del territorio nacional y en el ámbito del territorio de

un Estado obligado por el Convenio Europeo [el Convenio 108, Estrasburgo 1981, del Consejo de Europa] (art. 12).

4) comunicar, *revelar datos* sin estar autorizado para ello (art. 15).

9. CONCLUSIONES

1. La información sobre una persona (el conjunto de sus llamados, en un sentido muy amplio, *datos personales*) constituye una especie de «*duplicado*» de la persona misma, su apariencia o configuración ante los demás, la realidad virtual con la que resulta, generalmente, identificada. Por eso, proteger los datos de una persona es proteger a la persona misma, defender sus derechos esenciales, los derechos de la personalidad.

2.A. La esencial *dignidad* de la misma condición humana constituye el fundamento de los llamados *derechos de la personalidad* [cuyo derecho/raíz podría llamarse el derecho «a» la personalidad, el genérico derecho de cualquier persona al libre desarrollo de su mismidad]. Entre los derechos de la personalidad se cuentan: 1) el derecho al «honor» [esto es, el derecho al respeto al honor, o sea, al prestigio social que «por sus obras, por su linaje o por el grupo del que forma parte» a no ser injuriado, a no ser ofendido en la autoestima que de la propia dignidad de la persona deriva]; 2) el derecho a la «dignidad» [esto es, el derecho al respeto a la representación iconográfica de sí mismo]; 3) el derecho a la propia «imagen» [esto es, el derecho al respeto a la representación iconográfica de sí mismo]; 4) el derecho a la inviolabilidad de domicilio; etc.

2.B. Los derechos de la personalidad, también llamados derechos humanos o fundamentales, a medida que la sociedad ha ido evolucionando, se han ido ampliando, multiplicando. Nos hallamos ahora ante lo que se ha llamado *la «tercera generación» de derechos fundamentales* de la persona, que se pueden calificar como los derechos del Estado de Cultura propios de una sociedad informatizada: debe encuadrarse en ellos *el derecho a la intimidad*.

3.A. La intimidad es un término ambivalente. Significa confianza, confianza profunda, verdadera, nacida de muy dentro. Significa también reserva, escondimiento de algo que se queda dentro, en el interior de la persona, que no se manifiesta a nadie: si acaso, precisamente sólo se manifiesta a las personas «de confianza». El derecho no puede garantizarnos la *intimidad/confianza* respecto a nadie. El derecho puede protegernos la *intimidad/reserva* frente a cualquiera que la violente, que la invada o trate de invadirla, que se inmiscuya en lo que es nuestra «reserva» (en la reserva de nuestro inviolable domicilio, en la reserva de nuestros inviolables datos personales).

3.B. Una manifestación [o una derivación] del derecho a la intimidad, o derecho a la vida privada, es el derecho al control de la información sobre sí mismo o *el derecho a la inviolabilidad de los datos nominativos*, como es preferible que se diga:

a) porque, atendiendo a su evolución histórica, de la institución jurídica de la inviolabilidad del domicilio deriva la construcción [doctrinal, primero, y jurisprudencial después] del derecho a impedir la información sobre sí mismo, deriva la figura de la inviolabilidad de los datos personales;

b) porque, atendiendo a su naturaleza jurídica, la inviolabilidad de datos tiene significación semejante a la inviolabilidad de domicilio: un atentado a la intimidad de la persona, una inmisión ilícita en su vida, se produce cuando se violenta el recinto cerrado de su domicilio y también cuando se violenta el recinto cerrado de la información sobre sí mismo].

4. La expresión «*Protección de datos*» la empleamos con el significado de «*Medidas legislativas que, [a] para proteger el reconocido por la generalidad de las Constituciones políticas derecho a la dignidad y a la intimidad [en un sentido muy amplio] de las personas físicas [no debería hacer falta la redundancia], [b] regulan [en definitiva, limitan, reprimen] la actividad humana que consista en la recogida, la elaboración o la difusión de datos personales nominativos por medio de aparatos que funcionen automáticamente. Constituyen leyes de Protección de Datos, y han sido objeto de nuestro análisis, las de los países siguientes: Alemania (de 1977); España (de 1992); Francia (de 1978); Gran Bretaña (1984).*

5. Pese a la particularidad de las respectivas distribuciones sistemáticas de su articulado, *el conjunto de la Leyes analizadas incorporan un repertorio común de cuestiones que, aventurándonos a una ordenación ideal, podrían enunciarse así:*

1) **DISPOSICIONES GENERALES** y definiciones legales. (Convendría incluir en esta cuestión un apartado específico dedicado a determinar el contenido de los ficheros objeto de la Ley de Datos, *el alcance de la Ley (?)*, su «entorno operativo», qué tipo de ficheros se incluyen o se excluyen del régimen [protector/represor] de la Ley en cuestión. Es algo que las Leyes dicen de pasada y no muy expresamente; salvo la Ley Inglesa, que dedica una Parte de su Texto a Exenciones (Art. 26 y ss.).

2) **RÉGIMEN LEGAL** de la constitución y del funcionamiento de los ficheros de datos nominativos: a) de los ficheros de titularidad pública; y b) de los ficheros de titularidad privada.

3) **DERECHOS Y DEBERES**: referidos [sobre todo, los derechos] al sujeto titular de los datos (el «interesado») y [sobre todo, los deberes] al sujeto titular del fichero de datos (el «titular del fichero»).

4) **ÓRGANOS DE PROTECCIÓN** de los datos (se llamen como se llamen: Comisario, en Alemania; Agencia, en España; Comisión [etc.], en Francia; Registrador, en Gran Bretaña).

5) **INFRACCIONES Y SANCIONES.** (En punto al *procedimiento judicial* para la Protección de Datos no hay un planteamiento uniforme: la única que instituye un procedimiento específico a utilizar y un específico Tribunal al que acudir para la Protección de Datos es la Ley Inglesa, art. 3 y Anejo II, Parte II).

6. En el ámbito de las definiciones vienen a coincidir las cuatro Leyes en usarse de estos cinco términos:

1) **DATOS** de tipo personal [podemos adoptar la expresión, con base en la Ley Francesa, de *informaciones nominativas*, o «datos nominativos».

2) **INTERESADO**, titular de los datos nominativos, «concernido», afectado o como con cualquier otro nombre se le llame [«Data sujet» le llama la Ley Inglesa].

3) **FICHERO DE DATOS** [«conjunto de datos» «memoria informatizada», ¿banco de datos?; el término «fichero/banco» podría valer como denominación genérica dentro de la que caben las especies de «archivos» y las subespecies de «registros»: un registro equivaldría a una ficha personal, a un «fichero/documento» electrónico con los datos de una determinada persona].

4) **TRATAMIENTO DE DATOS.** Se designa con este término las operaciones, generalmente automatizadas, que se llevan a cabo sobre los datos nominativos y que, en un intento de dar a la palabra «tratamiento» la máxima extensión posible, incluye la *recogida* de datos, pasa por su *elaboración* o tratamiento propiamente dicho y abarca la misma *difusión*, transmisión o comunicación de los datos. Los textos legislativos usan el término «tratamiento» como una reminiscencia de la misma definición de informática (tratamiento de la *información* por procedimientos *automáticos*). Pensamos que la expresión «procesar información» es más precisa (y tan usual o más) que la expresión «tratar información». Podría, por tanto, imponerse el neologismo de «procesamiento» de información; y hablar, mejor que de datos «tratados», de datos «procesados», o aun de datos [y, en su caso, ficheros] «informatizados».

5) **TITULAR** del fichero de datos personales: tal es el término, a nuestro parecer, más aceptable; preferible a «entidad almacenadora de datos» (de la Ley Alemana), a «responsable del fichero» (de la Ley Española), a «dueño/administrador» de los datos [Data user] (de la Ley Inglesa). El titular del fichero es quien puede disponer de él, de su constitución y funcionamiento.

7. Respecto a los principios, las Leyes (llamadas a la efectiva aplicación de los mismos) recogen a su modo los Principios del Convenio de Estrasburgo,

que se quedan a medio camino entre lo que son *principios generales* propiamente dichos [ideas madre] y lo que son *específicos deberes* de los administradores o titulares de los ficheros automatizados de datos personales. Caben muchas y muy heterogéneas ideas/madre a la hora de pensar en la protección de datos: Legalidad de actuaciones, Veracidad de la información (o acaso Cualificación de datos), Indemnización de perjuicios causados al sujeto titular de los datos, etc. No siguen las Leyes analizadas un criterio uniforme a la hora de formalizar los principios que inspiran sus preceptos. Con todo, los principios fundamentales de la protección de datos que prácticamente se repiten en las disposiciones legislativas analizadas pueden sintetizarse en esta especie de cinco mandamientos laicos:

1) *El primero, NO TOMAR los datos ajenos sin el consentimiento de su dueño, es decir, del interesado; éste deberá ser INFORMADO* previamente de la finalidad y condiciones de la toma de datos ; (y, si fueron tomados y almacenados, el que los tenga deberá MOSTRARLOS [exhibirlos] cuando el interesado ejercite su derecho de «acceso»; y aun, si fuere preciso, RECTIFICARLOS o CANCELARLOS a petición del interesado).

2) *El segundo, CUMPLIR lo que mande la autoridad protectora de datos.*

3) *El tercero, CUSTODIAR con esmero el fichero de datos: tomar las necesarias medidas de seguridad para la protección de los datos.*

4) *El cuarto, NO MOSTRAR a terceros los datos (no decir ningún dato a terceros, no revelarlos fuera de los casos en que la revelación esté legitimada).*

5) *El quinto, CANCELAR, BORRAR para siempre, los datos «prescritos», caducos, pasados de tiempo.*

En suma: 1) Disponibilidad privada, 2) Intervención pública, 3) Seguridad, 4) Confidencialidad y 5) Olvido.

8. En cuanto a las infracciones, el tratamiento que las Leyes hacen de ellas no es ciertamente uniforme. Hay en este punto reglamentaciones prolijas (como la Española, que recoge 23 supuestos de infracción de la Ley), y más escuetas (como la Alemana, que recoge solamente 6 supuestos). Las sanciones consisten, unas veces, en sólo multas, como en el caso de Gran Bretaña; y, otras veces, en sanciones penales combinadas con multas más o menos cuantiosas. Dónde esté la ideal sanción, la más eficazmente disuasoria, es asunto opinable: las multas excesivas tienen el riesgo de no poder ser cumplidas, y las pequeñas no intimidan lo suficiente; la confiscación de ficheros, y aun la inhabilitación profesional de los infractores, si llega el caso, pueden ser medidas sancionadoras convenientes.

9. Son muchas las cuestiones que un análisis de cualquier texto legislativo remueve. La Protección de datos se debiera inscribir en un planteamiento, más

amplio y progresista, en lo que constituye, al decir de Frosini, el nuevo Derecho de la información; que comprendería: 1) el derecho a *recibir* información (a estar informados de todo cuanto, en un sentido muy amplio, pueda resultar de nuestro interés); 2) el derecho a *emitir* información; y 3) el derecho a *controlar* la información sobre nosotros, a la inviolabilidad de datos nominativos (IDNI). Aun para proteger este derecho a «controlar» la información sobre nosotros cabe una política «educativa» de difusión de la información.