EL DERECHO A LA INTIMIDAD, LA VISION IUSINFORMATICA Y EL DELITO DE LOS DATOS PERSONALES

Dr.
Antoni Monreal Ferrer
Director de Tesis

Tesis para optar el título:
Doctor en Derecho
Universidad de Lleida (España).

Por:
Libardo Orlando Riascos Gómez

UNIVERSIDAD DE LLEIDA
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PUBLICO
Lleida (España), 1999

EL DERECHO A LA INTIMIDAD, LA VISION IUSINFORMATICA Y EL DELITO DE LOS DATOS PERSONALES

Dr. Antoni Monreal Ferrer
Director de Tesis

Por:
Libardo Orlando Riascos Gómez

UNIVERSIDAD DE LLEIDA
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PUBLICO
Lleida (España), 1999

ABREVIATURAS Y SIGLAS

Art.	Artículo (Leyes o decretos-leyes o AAct@ anglosajona)
BOE	Boletín Oficial del Estado Español
CE	Constitución Española de 28 de Diciembre de 1978
Cons.Pol.	Constitución Colombiana de 7 de Julio de 1991
C.C.	Corte Constitucional de Colombia
C.C.A.	Código Contencioso Administrativo Colombiano de 1984-1989
CC	Código Civil Colombiano
C.P.	Código Penal de Colombia de 1980
C.P.Esp.	Código Penal de España de 1995
DANE	Departamento Administrativo Nacional de Estadística de Colombia.
Decr.	Decreto-Ley de Colombia
DNI	Documento Nacional de Identidad en España
DIN	Documento de Identidad o Cédula de ciudadanía en Colombia
DO	Diario Oficial del Estado Colombiano
D.R.	Decreto Reglamentario en Colombia
EDI o IED	Electronic Data Interchange o Intercambio electrónico de datos
E-Mail	Correo electrónico
E/S o I/O	Entrada/Salida de señales de comunicación
HTML	Hypertext Markup Language o simplemente Hipertexto
htttp	Hypertext Transfer Protocol
LDPIC	Ley de Protección de la Intimidad del Canadá o APrivacy Act@ 1988
LAIC	Ley de Acceso a la Información del Canadá o AAcces to Information Act@
LPIDA	Ley de Protección de la Intimidad y de los Datos personales en Australia o APrivacy and data Bill 1994 (NSW)@.
LFAPD	Ley Federal Alemana de Protección de Datos de 1997-1990
L.O.	Ley Orgánica de España
LORTAD	Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal de 29 de Octubre de 1992.

LRJPA	Ley de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo común de 29 de Noviembre de 1992
M.E.	Memoria Explicativa de la L.O., leyes, Convenio Europeo o Directiva.
MODEM	Modulador y Demodulador de señales de comunicación
OCDE	Organización de Cooperación y Desarrollo Económico de 1948
R.(Núm)	Numeral en la Recomendación de la OCDE de 1980
R.D.	Real Decreto Español.
RDSI	Red Digital de Servicios Integrados (En Directiva 97/66/CE).
Sent.	Sentencia de los Tribunales Colombianos
STC o SSTC	Sentencia o sentencias del Tribunal Constitucional de España
TC	Tribunal Constitucional de España
TIC	Tecnologías de la Información (TI) y la Comunicación.
UE	Unión Europea o Comunidad Europea
URL	Uniform Ressource Locator. Sitio o Dirección Electrónica en la WEB.
WWW	Word Wide Web. Red de Redes de información, a través de las páginas de hipertexto o hipermedia.

DEDICATORIA

A mis amados padres: Cecilia Tirza y Pablo Elías (q.e.p.d.),
Quienes hicieron que surja en mi toda posibilidad, tarea e ideal.

A mis queridos hijos: Xabier, Nícolas y Gisela,
A mi gran amor: Vilma Olivia,
Con quienes lo posible es tiempo y es espacio...es obra.

ABSTRACT

The present constitutional juridical Rehearsal, has as primordial objectives, the study, analysis and theoretical and practical positions, on which call A*vision iusinformática*@ of the rights and fundamental freedoms, and in particular, the one of the right to the intimacy, with incidence in the administrative and penal public right. To such effects, we take as starting point, the interpretation hermeneutic of the Rehearsal written in 1890 by Samuel Warren and Louis Brandeis, entitled AThe Right to Privacy@, the Universal Declaration of Human Rights of December 10 of 1948; then, the comparative analysis of the international juridical norms (San José=s Pact, The Pact of New York and the Resolution of the OECD of 1980, have more than enough prosecution of personal data and right to the intimacy), the European Community norms (The Agreement of Rome has more than enough Human Rights of 1950, The Agreement of Strasbourg 1981, the Directive 95/46/CE and 97/66/CE, have more than enough computerized treatment of personal data and right to the intimacy), the state juridical norms of protection of data of personal character when they have been subjected to computer, electronic or telematic prosecution for juridical people, naturlaes, public or private (mainly, The German Law of 1977, the Australian Law AThe privacy and Dates protecction Bill of 1994 -NSW -@ and the Organic Law of Spain, about personal data and intimacy --LORTAD of October 29 of 1992--). And, finally, the punctual revision of the doctrinal positions and jurisprudence in Spain, Germany, Colombia, Italy and United States, on the call ANew Right@ of the A*Libertad Informática*@ --computer freedom-- (or computer self-determination, intimacy computer science, habeas data).

ABSTRACT

El presente Ensayo jurídico constitucional, tiene como objetivos primordiales, el estudio, análisis y planteamientos teóricos y prácticos, sobre la que llamamos Avisión iusinformática@ de los derechos y libertades fundamentales, y en particular, la del derecho a la intimidad, con incidencia en el derecho público administrativo y penal. A tales efectos, tomamos como punto de partida, la interpretación hermenéutica del Ensayo escrito en 1890 por Samuel Warren y Louis Brandeis, intitulado AThe Right to Privacy@, la ADeclaración Universal de Derechos Humanos de 10 de Diciembre de 1948"; luego, el análisis comparativo de las normas jurídicas internacionales (El Pacto de San José, El Pacto de New York y la Resolución de la OCDE de 1980, sobre procesamiento de datos personales y derecho a la intimidad), las normas comunitarias europeas (El Convenio de Roma sobre Derechos Humanos de 1950, El Convenio de Estrasburgo de 1981, la Directiva 95/46/CE y 97/66/CE, sobre tratamiento informatizado de datos personales y derecho a la intimidad), las normas jurídicas estatales de protección de datos de carácter personal cuando han sido sometidos a procesamiento informático, electrónico o telemáticos por personas jurídicas, naturlaes, públicas o privadas (principalmente, La Ley alemana de 1977, la Ley Australiana AThe privacy and Data protecction Bill de 1994 -NSW-@ y la Ley Orgánica de España, sobre datos personales e intimidad --LORTAD de Octubre 29 de 1992--). Y, finalmente, la revisión puntual de las posiciones doctrinales y jurisprudenciales en España, Alemania, Colombia, Italia y Estados Unidos, sobre el llamado ANuevo Derecho@ de la Alibertad informática@ o Aautodeterminación informática@, Aintimidad informática@, @habeas data@.

TABLA DE CONTENIDO GENERAL

PARTE I

CONCEPTUALIZACION DE LA VISION IUSINFORMATICA DE LA INTIMIDAD

PARTE II

LA VISION IUSINFORMATICA DEL DERECHO A LA INTIMIDAD, NO ES UN NUEVO DERECHO FUNDAMENTAL

PARTE III

LA IUSINFORMATICA Y LOS DATOS PERSONALES EN EL PROCEDIMIENTO INFORMATICO, ELECTRONICO Y/O TELEMATICO

PARTE IV

LA VISION IUSINFORMATICA DE LA INTIMIDAD EN LAS NORMAS PENALES. EN PARTICULAR, LA PROTECCION JURIDICO-PENAL DE LOS TITULARES DE DATOS PERSONALES REGISTRADOS EN AFICHEROS@ EN LOS LLAMADOS DELITOS DE LOS DATOS PERSONALES

INTRODUCCION

Hoy en día, el derecho a la intimidad personal y familiar, así como el conjunto de derechos y libertades fundamentales elevados a rango constitucional en la mayoría de Constituciones democráticas de los Estados Sociales de Derecho en las llamadas *sociedades informatizadas* de finales del siglo XX, han recibido un importante como cualificado soplo revitalizador en el constante y permanente cambio previsible y devenido en el procedimiento evolutivo de su conceptualización. Ese soplo impulsor; para la gran mayoría, o de efecto de grave peligrosidad, para otros, está dominado por las nuevas tecnologías de la información y la comunicación (TIC), a través de los medios y aplicaciones computarizados: electrónicos y telemáticos, en el ámbito del derecho público ha generado un fructífero discurso constitucional que pretende demostrar; por un lado, la comprobación de la teoría de escíndencia de nuevos derechos fundamentales, a partir de las visiones, facetas o bastiones preexistentes de otros derechos constitucionales de igual estirpe, tal como le sucede, en la doctrina y jurisprudencia iuspublicista españolas al interpretar el art. 18.4 CE, referente al derecho de la intimidad y la tutela de la inviolabilidad de la persona humana por el A*uso de la informática*@ como visión iustecnológica de aquél y; de otro lado, la corroboración de dicha visión o faceta del derecho a la intimidad, sin necesidad de engendrar uno nuevo a partir de ésta y con el consiguiente resultado de protección del ser humano con derechos fundamentales integrales que muestran su porosidad a todos los cambios sociales, políticos, culturales, científicos y sobre todo, de índole tecnológica, como los TIC que en términos de *Ethain Katsch*, proyectan en esta civilización de la información fuertes impactos en nuestra actual *cultura electrónica*, tal como lo hizo en su momento histórico la cultura tradicional de la escritura y la imprenta.

En este último sentido el derecho a la intimidad (o *The Right to Privacy* anglosajón) es un derecho integral con diferentes facetas devenidos de los diversos cambios, el último producido en la sociedad informatizada por las nuevas tecnologías TIC y la informática. Así, en la Constitución Española (art.18 CE) y en la Constitución Colombiana de 1991 (art.15), como en el Código Penal Español de 1995 que tutelan el derecho a la intimidad personal y familiar y sus principales facetas o bastiones.

Que duda cabe, que esta investigación socio-jurídica, por lo expuesto constituya un ensayo constitucional que apunta por la integralidad de los derechos fundamentales, a partir de esa cualidad o característica de alta porosidad que identifica a los derechos constitucionales denominados de A*tercera generación*@ no por engendrar nuevos derechos, entre otras razones, al abrigo de las *liberties pollution* sino por presentar a los derechos preexistentes de una forma nueva, remozados, transformados en su aspecto, a través de su enriquecimiento visional. La visión iusinformática de los derechos fundamentales y, en particular, del derecho a la intimidad, es una nueva visión o faceta de aquél derecho que ha sido posible por la permeabilidad y asimilación frente a los nuevos fenómenos tecnológicos TIC y la informática. El nexo lógico del *ius* (o jus) con la informática, crea la *iusinformática* como una mixtura posibilitada desde el momento mismo en que los juristas como *Lee Loeviger* en 1949, evidenció las ventajas de la ciencia del tratamiento lógico y concatenado de la información con fines preestablecidos (informática) aplicada al derecho. La Jurimetría sienta las bases de dicho nexo en la obra: *Jurimetrics: The next step forward*. Quizá por esto, los juristas comenzaron a estar cada día más comprometidos con la potenciación de ese nexo, pese o gracias a aquello. En esta investigación damos un medio paso más por el nexo.

El ensayo constitucional esta dividido en cuatro partes, a saber: La primera: *La Conceptualización de la visión iusinformática de la intimidad*. Esta se presenta la configuración, características, límites y proceso de conceptualización de la visión iusinformática del derecho a la intimidad extractados, a partir del recorrido doctrinal, jurisprudencial y legislativo del derecho público estatal español, colombiano, alemán y australiano, así como también del conjunto de normas de ámbito universal, internacional y comunitario europeo sobre derechos humanos y, en particular, sobre el derecho a la intimidad (The *Right to Privacy*) y los ordenamientos jurídicos que protegen a los titulares de los datos de carácter particular.

La Parte Segunda: *La visión iusinformática del derecho a la intimidad, no es un nuevo derecho fundamental*. Nos ubicamos con ello dentro de la postura negativa al nacimiento de un nuevo derecho fundamental denominado indistintamente: *Libertad informática, autodeterminación informática, intimidad informática, habeas data o habes scriptum,* a partir de una faceta o bastión tecnológico del derecho a la intimidad: la inviolabilidad de la persona humana por el Auso de la informática@. La visión iusinformática del derecho a la intimidad esta compuesta por una serie de principios, valores y facultades de otros derechos que sin llegar a desvirtuar, limitar o esfumarlos toman de estos sus potencialidades (v.gr. La inviolabilidad y el libre desarrollo de la persona, la dignidad, los derechos al control de la información, de oposición al tratamiento informatizado de datos personales, etc), cara a revitalizar la integralidad del derecho que le sirve de base o del cual se deriva.

La Parte Tercera: *La iusinformática y los datos personales en el procedimiento informatico, electrónico y/o telemático.* Presenta las fases, ciclos o etapas del procedimiento informático, extractadas del estudio y análisis de las diversas normas jurídicas estatales (v.gr. LORTAD de 1992 de España, Privacy and Data Bill 1994 de Australia, Ley Alemana de 1977-1990), internacionales (La Recomendación de la OCDE de 1980) y comunitarias europeas (Convenio de Estrasburgo de 1981 y la Directiva 95/47/CE) que regulan el tratamiento informatizado (que no simple y primigenia mente Aautomatizado@) de datos (entendidos como unidades lógicas de información digitalizada) personales, a través de medios informáticos, electrónicos o telemáticos.

La Parte Cuarta: *La visión iusinformática de la intimidad en las en las normas penales, la protección jurídico-penal de los titulares de datos personales registrados en Aficheros@ en los llamados delitos de los datos personales.* Sin perder el hilo conductor del discurso constitucional de la visión iusinformática que tiene validez en todos los ámbitos del derecho, y por supuesto en el penal, analizamos el estado actual del llamado Adelito informático@ en normas españolas y colombianas, con el sólo propósito de demostrar la integralidad de un derecho único: la intimidad, con diversas visiones o facetas. Especialmente, analizaremos la intimidad como bien jurídico constitucional y como derecho fundamental, objeto y sujeto de tutela iuspenalista en el Título X, Libro II del Código Penal Español de

1995 art..197, referente a los atentados contra la intimidad de las personas cuando se utiliza medios informáticos, electrónicos o telemáticos. A título de ensayo se propone la configuración del *delito de datos personales,* atendiendo a las fases del procedimiento informático y haciendo incapié en las que mayor vulnerabilidad y/o protegibilidad presentan actualmente en la sociedad informatizada en la que vivimos: las etapas de recolección y de comunicación de datos.

Primavera de 1999, Lleida (Esp.)

PARTE I

CONCEPTUALIZACION DE LA VISION IUSINFORMATICA DE LA INTIMIDAD

1. NOTAS PRELIMINARES

El Derecho a la intimidad en las Constituciones democráticas de la segunda mitad del presente siglo, ha sido considerado como un derecho fundamental del ser humano que hunde sus raíces en valores constitucionales como la dignidad humana, el respeto mutuo, el libre desarrollo de la personalidad y en el conjunto de principios y atribuciones que definen a la persona en nuestra sociedad actual y hacen parte de lo que hoy constituye un Estado Social de Derecho. Así se plasma en las Constituciones de España de 28 de Diciembre de 1978, art. 18 (CE) y en la Constitución Política de Colombia de 7 de Julio de 1991, art. 15 (Cons.Pol.) [1]. Nuestra investigación estudia tan solo la visión iustecnológica del derecho a la intimidad personal y familiar.

La proceso de evolución conceptual, tanto de la intimidad, como de los actuales derechos fundamentales [2] y del Estado mismo , --a riesgo decir un pleonasmo-- son

---

(1) El derecho a la intimidad desde la Centenaria Constitución Colombiana de 1886, constituía un derecho inherente a la persona humana y como tal inalienable, inenajenable e imprescriptible, pero indefectiblemente unido al concepto y abrigo del derecho a la honra de las personas. El art. 16 de dicha constitución establecía que las Autoridades legalmente instituidas en la República protegen y garantiza la Ala vida, honra y bienes@ de las personas. Los Tribunales y la Corte Suprema Colombianos, durante un siglo aplicaron la norma en el amplio campo de la responsabilidad extracontractual del Estado y en la teoría de ampliación y nacimiento de nuevos derechos de orden constitucional, como el de la intimidad, el libre desarrollo de la personalidad, la honra, la paz , el *habeas data*, etc (hoy, derechos fundamentales en la Constitución de 1991, arts. 15, 16, 21, 22 y 15 *in fine*, respectivamente). Vid. Mi trabajo, *LA CONSTITUCION DE 1991 Y LA INFORMATICA JURIDICA*. Ed. Universidad de Nariño, ENED, Pasto, 1997, pág. 25 y ss.

(2) Pretendemos, hacer énfasis en que todo proceso evolutivo de una institución, fenómeno o concepto socio-jurídico, no es producto de una generación espontanea sino de un difícil, lento y casi tortuoso parto que dura años o Asiglos@, y que hoy lo acogemos, sin beneficio de inventario, para tener un punto de partida seguro, y si cabe dentro de la lógica jurídica, un punto de apoyo decantado, pero no absoluto, en tanto en cuanto hace referencia al proceso de evolución conceptual de los que hoy denominamos Aderechos fundamentales@ por tener como referente a la persona humana en su vida, desarrollo y en su dignidad, así como a la interiorización del concepto en la sociedad actual y su consecuente plasmación en las Constituciones Políticas de cada Estado. Pretendemos igualmente, partir de los conceptos ya decantados por los constitucionalistas sobre el derecho a la

intimidad, sus principales características, en la estructuración del contenido esencial, el análisis de la teoría de los límites e incluso en las diferentes visiones o formas de cognoscibilidad en el mundo jurídico, para centrarlos en una visión en particular, la que denominamos la visión iusinformática de la intimidad. Sin perjuicio de volver sobre estos aspectos ampliamente discernidos en la doctrina, jurisprudencia y legislación española, con el sólo propósito de estructurar, reforzar y validar nuestra tesis de la mencionada visión del derecho a la intimidad. Véase, especialmente los comentarios del surgimiento y evolución del artículo 10 de la CE, catalogado como Apiedra angular de todo el sistema jurídico que ella (CE) instituye@, pues junto al análisis y evolución del art. 18.4 CE., constituyen el epicentro del presente ensayo constitucional en entronque con otras áreas jurídicas e informáticas. RUIZ-GIMENEZ CORTEZ, Joaquín. *EL ARTICULO 10*. En: COMENTARIOS A LA CONSTITUCION ESPAÑOLA DE 1978. Cortes Generales. Ed. Derecho Unidos. Madrid 1997, p.39 y ss.

fruto de una incesante e inacabada teorización basada en las prácticas, usos, costumbres y regulaciones normativas de los diferentes pueblos de la tierra y, por su puesto, del trabajo intelectual de la doctrina y jurisprudencia iusuniversales. Por eso, *ad portas* del siglo XXI, hemos decantado al derecho de la intimidad personal y familiar como un derecho fundamental de la persona humana, elevado a rango constitucional como derecho autónomo pero limitado por otros derechos de igual jerarquía, por el ordenamiento jurídico y por una serie de intereses, valores y principios igualmente constitucionales; pero por sobre todo, se ha considerado también al derecho a la intimidad como un derecho digno de excelsa protección por parte del Estado y de los particulares mismos, ante los pluriofensivos riesgos jurídico-tradicionales así como los devenidos recientemente por los avances tecnológicos de la información y la comunicación (conocidos en las ciencias de la comunicación, como fenómeno TIC [3]) unidos a los porosos, penetrantes y complejos desarrollos de la informática, electrónica y telemática [4].

La informática [5] --que tendremos oportunidad de puntualizar en el transcurso

---

(3) Estas nuevas tecnologías TIC, que surgieron inicialmente de las denominadas por el profesor *Ethain Katsh*, Atecnologías de la información TI@, no son sólo aquellas Aque se llevan a cabo con los simples artefactos funcionales, sino que constituyen verdaderas nuevas formas de recibir y transmitir información de forma más interactiva y permite recoger, seleccionar, organizar, almacenar y transferir cualquier cantidad de información de un sitio a otro, sin frontera geográfica alguna y a velocidades y formatos electrónicos@. Quizá por estas amplias capacidades de transmisión electrónica (emisión/recepción) en la que se basan las nuevas tecnologías de la comunicación , es por lo que estos fenómenos pueden calificarse de novísimas tecnologías TIC, adicionando a ese bien intangible, poderoso, poroso, penetrante, de difícil control (jurídico, tecnológico, personal y social) y de incalculable valor económico como es la *información* actualmente, el vehículo electrónico idóneo, sin el cual aquella pierde parte de su magia y estructuración, como lo es, la comunicación a través de medios eléctricos, informáticos, electrónicos y telemáticos. Mi Trabajo. LA CONSTITUCION.... Ob.ut supra cit., pág. 7 y ss. Vid. KATSH, Ethain. *RIGHTS, CAMERA, ACTION: CYBERSPATIAL SETTINGS AND THE FIRTS AMENDMENT*. Profesor of Legal Studies, University of Massachussetts at Amberst; B.A. 1967, New York Universiity; J.D. 1970, Yale University. Texto Original en inglés en la dirección electrónica: *WWW.UMONTREAL.EDU.CA.*

(4) El estudio pormenorizado de los soportes, medios y aplicaciones informáticas, electrónicas y telemáticas; así como, los impactos sociales, jurídicos y tecnológicos en la sociedad de la información en que vivimos serán tratados a profundidad y especio en la Parte III y IV., de esta investigación.

(5) *Vittorio Frosini* (En: Informática y Derecho), comenta como surgió el término Ainformática@ de la definición dada por *Philippe Dreyfus*, en los siguientes términos: AL´informatique est la science du traitement rationnel, notamment para machines automatiques, de l´information considerée comme le support des connaissances et des communications dans les domaines technique, économique et social@. Y fue también a partir de esta concepción de informática, que las diferentes Leyes de Protección de los Titulares de los Datos Personales en la Unión Europea (UE), como en los diferentes Estados que la componen, que se hizo institucional el término de A*tratamiento automático*@ de la información o datos de carácter personal, tal como tendremos oportunidad de profundizar más adelante. Terminología técnico-jurídica que aún subsiste, a pesar de corresponder a la etapa de surgimiento de la computación y de los ordenadores donde se destacaba una de las funciones primarias de aquellas máquinas, cual es, la automatización de datos, tal como lo hace hoy un cajero electrónico. Mi trabajo. *LA CONSTITUCION DE 1991 Y LA INFORMATICA JURIDICA*... Ob. cit., pág. 47 y ss.

de esta investigación--, se ha entendido, como la capacidad potenciada con medios informáticos, electrónicos y telemáticos (v.gr. elementos, aparatos y sistemas computacionales y de comunicación electrónica: la telemática y la multimedia) utilizados en el tratamiento logicial o mediante sistemas de tratamiento de **E**ntrada (E: ***I****nput*) o **S**alida (S: ***O****utput*) de cualquier cantidad o clase de información [6] generada por el ser humano en sus diversas actividades o profesiones. Información, en tanto en cuanto, sea considerada como un bien con valor económico [7], social y jurídico y sea posible transferirla (emitir y recepcionar) de un lugar geográfico a otro, a velocidades, con equipos y formatos eléctricos y electrónicos (comunicación por cable y electrónica [8]: telemática y multimedia [9]) y posean una finalidad y objetivos predeterminados.

La informática jurídica o *iusinformática*, hace referencia al tratamiento lógico, con soportes, equipos y medios eléctricos y electrónicos de la información o datos generados por el hombre en el ámbito social y jurídico.

La iusinformática es entonces, una parte especializada de carácter académico y sectorial de la informática general que día a día cobra capital importancia, porque a ella hay que referirse en la aplicabilidad de una coherente técnica legislativa con los nuevos fenómenos tecnológicos TIC y la informática tales; entre otros, como: a) En la regulación de los derechos y obligaciones consecuentes de la creación, distribución, explotación y/o utilización del hardware y software, con su protección en los derechos de propiedad industrial o en los propiedad intelectual; b) En la regulación de los derechos y obligaciones de los creadores, distribuidores y usuarios de bases de datos

---

(6) LOPEZ MUÑIZ-GOÑI, Miguel. *INFORMATICA JURIDICA DOCUMENTAL*.Ed. Diaz de Santos, Bilbao, 1984, pág. 39. Citado en mi trabajo, *LA CONSTITUCION DE 1991 Y* ... Ob. cit., pág. 72 y ss.

(7) En el ámbito punitivo español siguiendo las tesis alemanas de Tiedemann, se propone la tesis de creación del bien jurídico denominado de la información, siempre que sea tenida como bien con valor económico, para referirse a los llamados delitos informáticos. Sobre este aspecto, profundizamos en la Parte IV., de esta investigación-ensayo. Vid. GUTIERREZ FRANCES, María Luz. *DELINCUENCIA ECONOMICA E INFORMATICA EN EL NUEVO CODIGO PENAL*.. En: Cuadernos de Derecho Judicial. Escuela Judicial. C.G.P.J. No. XI, Madrid, 1996. Además, *NOTAS SOBRE LA DELINCIENCIA INFORMATICA: ATENTADOS CONTRA LA AINFORMACION@ COMO VALOR ECONOMICO DE EMPRESA*. En: Estudios de Derecho Penal Económico. Editores: Luis Zapatero y klaus Tiedemman. Ed. Univ. de Castilla-La Mancha. Tarancon (Cuenca). 1994, pág. 183 a 208.

(8) KATSH, Ethain. Ob. ut supra cit., en la dirección electrónica *WWW.UMONTREAL.EDU.CA*.

(9) La multimedia es una de las formas de comunicación electrónica realizada a través de elementos, sistemas y equipos computacionales, por los cuales se transfiere (emite/recepciona) cualquier tipo de información o datos contenidos en formatos de texto, imágenes y sonido.

jurídicos (o A*ficheros*@, según la terminología francesa y española); c) En la contratación de bienes y servicios informáticos; d) En las ALeyes protectoras de Datos Personales@ y la potencial no sólo agresividad, sino defensabilidad que representa, según el caso la

informática; e) La estructuración y regulación normativa de los denominados A delitos

informáticos A [10]; f) la regulación del ejercicio, protección y garantía de los derechos y libertades fundamentales de la persona humana (Ael honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos@, art. 18.4 CE); y g) La regulación de los derechos estructurales del derecho de *habeas Data* (acceso, actualización, rectificación y cancelación), posteriores a los derechos de notificación e información (Aderecho a conocer@) que ostenta el titular de los datos que le conciernen en un sistema de tratamiento (recolección, almacenamiento, registro, conservación y Acirculación de datos@) informatizado y aplicable al conjunto de derechos y libertades fundamentales previstos en la Constitución Colombiana [11], la Portuguesa [12] y la

---

(10) Por éstos y otros supuestos que amplía la lista, es por lo que el Davara, estima que la iusinformática, hoy por hoy, bien puede configurar una nueva rama del derecho, el *Derecho Informático*, en el que todos los juristas estamos comprometidos a Atrabajar para colaborar en marcar bien claramente las diferencias entre lo que es, lo que puede ser y lo que debe ser, orientando el camino que debe tomar la regulación jurídica del fenómeno informático en la hemos dado en llamar el ADerecho Informático@. Nosotros creemos haber aportado algo a esa estructuración en el trabajo *ut supra* citado. DAVARA RODRIGUEZ, Miguel A. *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi S.A., Pamplona, 1997, págs. 25 a 41.

(11) La Constitución de 1991, en el art. 15, inmerso en el Título II, Cap.I., ADe los Derechos Fundamentales@, expresa: A Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetalos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución....@. Aunque el derecho de habeas data esta inmerso en el de la

intimidad, no debe interpretarse en forma miope que sólo a éste es aplicable, como tendremos oportunidad de puntualizar más adelante, con base en fallos de la Corte Constitucional Colombiana, sino que por la ubicación sistemática no simplemente formal, la garantía y protección constitucional se reputa para el conjunto de derechos considerados fundamentales. El error de la ubicación temática del habeas data por parte de la Comisión Codificadora de la Constituyente de 1990, no debe conducir a la negación o, más aún, la evaporación de las garantías y mecanismos constitucionales de protección del conjunto de derechos fundamentales. El Constituyente Colombiano debió beber íntegramente de las fuentes de donde transplantó parcialmente el art. 35 de la Constitución Portuguesa (que regula la AUtilización de la Informática@ en el contexto del Titulo II, Cap. I. ADereitos, libertades e garantias pessoais@), a fin de que no aparezca un artículo 15 (Derecho a la Intimidad) fusionado con el de habeas data y generando, --lo que es aún peor-- una forzada y casi inseparable dependencia.

(12) El Titulo II, Dereitos, Libertades e garantias, Cap.I, Art. 35 (Utilizaçâo da informática). Por la ubicación formal y sistemática del citado artículo se deduce que el derecho de habeas data como la limitación al uso de la informática se aplica al conjunto de derechos y libertades fundamentales. Citamos a continuación el texto normativo conforme a la reforma introducida al art. 35, según la LC Núm. 1/1982, pues el texto original de la Constitución de 1976 que constaba de tres numerales fue reformado, aunque el espíritu y gran parte del texto de aquella se mantuvo. La mentada norma expresa: 35-1. Todos los ciudadanos tendrán derecho a tener conocimiento de lo que consta en forma de registros informáticos que les conciernen y de la finalidad a la que se destinan esas informaciones (datos o registros), y podrá exigir, llegado el caso, la rectificación de los datos, así como su actualización. 35-2. Esta prohibido el acceso de terceros a los ficheros (o banco de datos) con datos personales o a la respectiva interconexión de aquéllos, a través de los flujos transfronterizos, salvo en las casos exceptuados en la ley (Inciso nuevo). 35.3 La informática no podrá ser utilizada para el tratamiento de datos referentes a las convicciones filosóficas o políticas, a la filiación partidista o sindical, a la fe religiosa o la vida privada, salvo cuando se trata de procesamiento de datos no identificables

Constitución del Brasil **[13]**.

Por la necesidad cada día mayor del derecho de regular materias del conocimiento humano, sobre todo las de índole tecnológico surgidas de la llamada informática, para que sean creadas, desarrolladas, protegidas, garantizadas y utilizadas conforme a un ordenamiento jurídico en vigor, es por lo que el profesor *Hernández Gil*, citado por *Davara* **[14]**, al hablar de los problemas socio-culturales de la informática jurídica, estima que el derecho *strictu sensu* no va a ordenar nuevas realidades, sino que el Derecho mismo va a experimentar, en cuanto objeto de conocimiento, una mutación, derivada de un modo distinto de ser elaborado, tratado y conocido. Sin embargo, dicha experimentación es de tal entidad que la informática necesita del derecho, como el derecho de la informática, tal y como lo sostienen *González Navarro* y *Lasso de la Vega* **[15]**, que resulta insuficiente la estricta observación pasiva de los juristas por lo que sólo la iusinformática puede aportar al derecho, si éste a su vez, no suministra sus técnicas, métodos y procedimientos que lo catalogan como ciencia social del conocimiento humano para comprender la dialéctica que se esta produciendo en su interior, tras el advenimiento de las nuevas tecnologías TIC en unión con la informática, hasta tal punto que, hoy hablamos de un *Derecho informático*, impensable décadas de años atrás.

Con sus limitaciones temporales y temáticas puntualizaremos estos temas.

--Continuación nota 12--
individualmente para fines estadísticos. 35-4. La ley definirá el concepto de datos personales para efectos de registro informático (nuevo). 35-5. Se prohíbe la atribución de un número nacional único a los ciudadanos. Los paréntesis de la norma son nuestros, así como los giros de traducción no literal del portugués. Texto Constitución Completo en: AA.VV. *CONSTITUÇAO NOVO TEXTO*. Coimbra editora, Ediçao organizado JJ. Gomes Conotilho o vital M., 1982

(13) Así lo confirman, los profesores *González Navarro y González Pérez*, siguiendo a *Heredero Higueras*, al recordar que la Constitución brasileña de 1988, incorporó el su texto el derecho de *habeas data* que inicialmente sólo se atribuía al derecho que tenía toda persona para acceder a la información que le concernía al considerarse Auna modalidad de acción exhibitoria análoga a la del habeas corpus@. Hoy en día, la estructuración y ampliación del contenido de aquél derecho, conlleva a extender las facultades iniciales de dicho derecho a otras, tales como los de actualización (o la puesta al día --*up date anglosajón*-- de los datos), rectificación y cancelación de los datos personales que le conciernen a una persona, sí los datos fueren inexactos, incompletos o ilegales. Vid. GONZALEZ NAVARRO, F. Y GONZALEZ PEREZ, J. *COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y PROCEDIMIENTO ADMINISTRATIVO COMUN*. Ed. Civitas, 1a., ed., Madrid, 1997, pág. 711.

(14) DAVARA RODRIGUEZ, Miguel. *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi Pamplona, 1997. pág. 21 y ss.

(15) Vid. GONZALEZ NAVARRO, Francisco. *DERECHO ADMINISTRATIVO ESPAÑOL*. Ed. Eunsa (Univ. de Navarra), Pamplona, 1987, pág. 190-194.

2. DIFERENTES CONCEPTUALIZACIONES DIVERSAS VISIONES DE LA INTIMIDAD.

El derecho a la intimidad personal y familiar, en la Constitución Española (como en la Colombiana), es un derecho fundamental protegido y garantizado por el Estado y los particulares, reglamentado en los diferentes estatutos normativos que persiguen, entre otros fines, la tutela efectiva de sus titulares y la garantía de su pleno ejercicio en las diversas órbitas jurisdiccionales: civiles **[16]**, contencioso-administrativas, penales **[17]** y constitucionales e incluso en ámbitos de competencia no judiciales, es decir, en vía administrativa (o Agubernativa@) y hasta en una vía *sui géneris* sancionatoria- administrativa desatada ante organismos independientes de los poderes públicos tradicionales v.gr. La Agencia de Protección de los Datos Española **[18]**.

---

(16) La moderna regulación del derecho a la intimidad en España, comienza con la expedición de la Ley Orgánica 1/1982, de 5 de mayo, que regula la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Esta ley desarrolla el art. 18.1 CE, que garantiza tres derechos fundamentales, incluido la intimidad. Aunque se piensa que el derecho a la imagen no es más que una manifestación corporal de la intimidad [v.gr. El Caso Marks Vs. Joffa. El Tribunal de New York Aplicó los conceptos jurídicos de la Aprivacy@ de Warren y Brandeis, en 1893 para darle razón al demandante cuando solicitaba tutela judicial por la

publicación de su imagen (fotografia) en un periódico sin su consentimiento. Aquí se tuteló el ARight to privacy@, por ser la imagen una emanación de la privacy], su autonomía persiste en la CE. La Exposición de Motivos (E.M.), explica el alcance y objetivos de la ley, así: A...el art. 20- 4 CE, dispone que el respeto de tales derechos (intimidad, honor e imagen) constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales... Establece el art. 1.1. de la misma la protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen frente a todo género de injerencia o intromisiones ilegítimas. Pero no puede ignorar que algunos de esos derechos gozan o previsiblemente gozarán de una protección penal. Así ocurre con el derecho al honor, amparado por las prescripciones contenidas en el libro II, título X, del vigente Código Penal, y con determinados aspectos del derecho a la intimidad personal y familiar que son objeto de una protección de esa naturaleza en el proyecto de nuevo Código Penal recientemente aprobado por el Consejo de Ministros. Por ello, en los casos que exista la protección penal tendrá ésta preferente aplicación, por ser sin duda la de más fuerte efectividad, si bien la responsabilidad civil derivada del delito se deberá fijar de acuerdo con los criterios que esta ley establece. Los derechos garantizados por la ley han sido encuadrados por la doctrina jurídica más autorizada entre los derechos de la personalidad, calificación de la que obviamente se desprende el carácter de irrenunciable, irrenunciabilidad referida con carácter genérico a la protección civil que la ley establece.@ Si bien esta ley tenía como objeto prioritario el desarrollo legislativo del art.18-1 CE, sobre el art.18-4, sostuvo: ADisposiciones transitorias.1. En tanto no se promulgue la normativa prevista en el art. 18-4 CE, protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley@. Texto completo en *AA.VV. COMPENDIO DE DISCOS COMPACTOS ARANZADI*. Ed. Aranzadi, 1997.

(17) A partir de la Expedición del Código Penal de 1995, se erigió como bien jurídico constitucional autónomo, el derecho a la intimidad personal y familiar, que antes había sido protegido y tutelado con carácter de *ultima ratio* en España, como derecho constitucional sí, pero dentro del bien jurídico (que para muchos iuspenalistas resultaba, cuando menos, poco conveniente, como veremos en la parte IV de este trabajo) denominado de la *Libertad y Seguridad de las personas.* Hoy, existe una dual protección punitiva del derecho a la intimidad: a) como bien jurídico autónomo, tutelado en el Libro II, Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio (arts. 197 a 204); y b) como derecho fundamental bajo otros bienes jurídicos: Delitos contra la Constitución: De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales (Tit. XXI. Cap. V). De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad (arts. 534 a 536).

(18) Vease, punto 4. 4, 4.4.3. y 4.4.3.1. Parte I.

El cuadro de protección y defensa del derecho fundamental de la intimidad, a partir del art. 18 CE, en España y el art.15 Cons. Pol., en Colombia, es tan amplio, como variado y regulado en forma pormenorizada en el ordenamiento jurídico vigente, a tal punto, que se conocen diversos niveles de protección: unos de tipo cautelar o preventivo, en vía administrativa; y otros, a nivel reparador e indemnizatorio en vías jurisdiccional civil y contencioso-administrativo; a nivel represivo o punitivo en el ámbito penal; y aún a nivel que podríamos llamar de protección *in integrum* en vía constitucional de *Arecurso de amparo@* **[19]**, en España, o mediante la *Aacción de tutela@***[20]**, en

---

(19) El Tribunal Constitucional de España, tiene jurisdicción en todo el territorio español y ante éste se ejercita el recurso de amparo por la violación de los derechos y libertades fundamentales (incluido la intimidad), en los casos y formas que establezca la ley (arts. 53-2 y 161.1.a CE). LEY ORGANICA 3-10-1979, núm. 2/19 (BOE 5-10-1979, núm. 239, [pág. 23186]). TRIBUNAL CONSTITUCIONAL. Modificado, arts. 50 y 86.1, por Ley Orgánica 9-6-1988. ***CAPITULO III. De la resolución de los recursos de amparo constitucional y sus efectos***. **Art. 53**. La Sala al conocer del fondo del asunto, pronunciará en su sentencia alguno de estos fallos: a) Otorgamiento de amparo. b) Denegación de amparo. **Art. 54.** Cuando la Sala conozca del recurso de amparo respecto de decisiones de los Jueces y Tribunales limitará su función a concretar si se han violado derechos o libertades del demandante y a preservar o restablecer estos derechos o libertades y se abstendrá de cualquier otra

consideración sobre la actuación de los órganos jurisdiccionales. **Art. 55.** 1. La sentencia que otorgue el amparo contendrá alguno o algunos de los pronunciamientos siguientes: a) Declaración de nulidad de la decisión, acto o resolución que hayan impedido el pleno ejercicio de los derechos o libertades protegidos, con determinación en su caso de la extensión de sus efectos. b) Reconocimiento del derecho o libertad pública, de conformidad con su contenido constitucionalmente declarado. c) Restablecimiento del recurrente en la integridad de su derecho o libertad con la adopción de las medidas apropiadas, en su caso, para su conservación. 2. En el supuesto de que se estime el recurso de amparo porque la Ley aplicada lesiona derechos fundamentales o libertades públicas, la Sala elevará la cuestión al Pleno, que podrá declarar la inconstitucionalidad de dicha Ley en nueva sentencia con los efectos ordinarios previstos en los artículos 38 y siguientes. La cuestión se sustanciará por el procedimiento establecido en los artículos 37 y concordantes. **Art. 56.** 1. La Sala que conozca de un recurso de amparo suspenderá, de oficio o a instancia del recurrente, la ejecución del acto de los poderes públicos por razón del cual se reclame el amparo constitucional, cuando la ejecución hubiere de ocasionar un perjuicio que haría perder al amparo su finalidad. Podrá, no obstante, denegar la suspensión cuando de ésta pueda seguirse perturbación grave de los intereses generales, o de los derechos fundamentales o libertades públicas de un tercero. 2. La suspensión podrá pedirse en cualquier tiempo, antes de haberse pronunciado sentencia o decidirse el amparo de otro modo. El incidente de suspensión se sustanciará con audiencia de las partes, y del Ministerio Fiscal, por plazo común que no excederá de tres días y con informe de las autoridades responsables de la ejecución, si la Sala lo creyera necesario. La suspensión podrá acordarse con o sin afianzamiento. La Sala podrá condicionar la denegación de la suspensión en el caso de que pudiere seguirse perturbación grave de los derechos de un tercero, a la constitución de caución suficiente para responder de los daños o perjuicios que pudieren originarse. Texto completo en *AA.VV. COMPENDIO DE DISCOS COMPACTOS ARANZADI*. Ed. Aranzadi, 1997.

(20) En el Derecho Constitucional se arbitran diferentes mecanismos constitucionales de control y protección de los derechos fundamentales (v.gr. La acción pública de inconstitucionalidad, la acción pública de nulidad). Uno de los más importantes y excesivamente utilizados, es la acción de tutela, por medio la cual Atoda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción u omisión de cualquier autoridad pública. La protección consistirá en una orden para que aquél respecto de quien se solicita la tutela, actúe o se abstenga de hacerlo. El fallo, que será de inmediato cumplimiento, podrá impugnarse ante el juez competente y, en todo caso, éste lo remitirá a la Corte Constitucional para su eventual revisión. Esta acción sólo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que aquélla se utilice como mecanismo transitorio para evitar un perjuicio irremediable. En ningún caso podrán transcurrir más de diez días entre la solicitud de tutela y su resolución. La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión@. (art.86). Los Decretos 2591/1991, de 19 de Noviembre y 306 de 1992, desarrollaron la norma constitucional. Texto completo, en: WWW. MINJUSTICIA. GOV.CO. (Base de Datos del Ministerio de Justicia de Colombia).

Colombia. Sin embargo, por ahora no son objeto de nuestra investigación, aunque vale la pena referenciarlos para entender el estado global actual de protección del derecho a la intimidad en España y en Colombia y poder dimensionar la particularidad específica de la protección de la intimidad, a través de la visión iusinformática.

Pese a ello, *Fariñas Matoni* [21] en 1983, consideraba que en España, la legislación para ese entonces vigente sobre el derecho a la intimidad era fragmentaria, anticuada, incompleta, asistemática, indirecta, esporádica e incidental, siendo deseable una nueva normativa actualizada y a la altura de los tiempos en que vivimos y que, sobre todo, vamos a vivir, y que contemple la cuestión: a), desde el punto de vista civil (el daño a la intimidad como modalidad especial del daño moral); b), desde el punto de vista penal, sancionando ciertos tipos de intromisiones;

c), desde el punto de vista administrativo y preventivo, para evitar que se produzcan ciertas situaciones o se adquieran determinados instrumentos nocivos al derecho a la intimidad. Muy pronto las fundadas críticas del autor citado se ha visto reducidas a su mínima expresión, pues el marco de protección actual del derecho a la intimidad esta a la altura de los Estados democráticos y consecuente con los adelantos tecnológicos TIC e informática.

Estos mecanismos de protección del derecho constitucional de la intimidad, antes referenciados, muestran el panorama garantísta constitucional y normativo tan frondoso como variopinto y cuasimilar que actualmente tiene el derecho a la intimidad en las dos legislaciones tipo (Española y Colombiana), lo cual hace impensable imaginar como hace más de un centenario desde que produjera el famoso precedente norteamericano, apartir del ensayo de A*Warren y Brandeis*@ se pudieran construir teorías, discursos constitucionales sobre la existencia o no de un derecho a la *privacy* o de mecanismos, procedimientos, Estatutos normativos e incluso elevarse a rango constitucional un derecho que bebe de las fuentes iusnaturalistas (dignidad de la persona humano) para convertirse en derecho positivo y más aún, en derecho fundamental del ser humano. El Derecho a la Intimidad, o en su origen angloamericano *The Right to Privacy*, surgió en una intromisión o injerencia periodística en la Aprivacy@ de un famoso personaje de la vida social y política norteamericana del siglo pasado en unos ambientes históricos, sociales, culturales, étnicos, políticos e incluso de concepción y estructuración, tan

---

(21) FARIÑAS M., Luis. *EL DERECHO A LA INTIMIDAD*. Ed. Trivium, S.A., Madrid, 1983, págs. 355 a 367.

disímiles en tiempo, espacio y aún conceptuales de lo que hoy entendemos en líneas generales por *privacy*[22] o por intimidad. Sin embargo, todavía hoy, estos aspectos de forma, ambientales y aún geográficos sirven de base para ampliar la conceptualización o manifestaciones de ese derecho único que es la Intimidad, pues el paso del tiempo nos ha servido para universalizar aquél derecho, para enriquecerlo con sus diferentes manifestaciones o visiones, para legalizar o constitucionalizarlo entre los Estados con derecho escrito como el Español y Colombiano, sin olvidar el

precedente angloamericano en sus orígenes, en su estructuración teórico-práctica y sus posibilidades de enriquecimiento con el paso de los años, los espacios geográficos o los avances tecnológicos, como los sobrevenidos a mediados del siglo XX y conocidos como TIC.

En tal virtud, para estructurar la visión iusinformática del derecho a la intimidad, partiremos del precedente norteamericano de 15 de diciembre de 1890 [23], pues a partir aquí se comienza a delinear *The Right to privacy*, como un derecho de la persona humana, diferente a los demás derechos existentes (patrimoniales o extrapatrimoniales), aunque retome elementos y características de algunos otros como el de propiedad, el derecho a la vida o valores constitucionales como la *inviolabilidad y dignidad de la persona* para explicarlo y estructurarlo, sin confundirlo con ellos. Así mismo, partimos del precedente, pues desde aquél entonces ya se vislumbraba la visión iustecnológica de la intimidad, cuando en las decisiones del Tribunales Norteamericanos recogidas en el Ensayo de Warren y Brandeis se proscribía *las injerencias en la privacy con aparatos fotográficos* (Acámaras de fotografía@) *o* producto de los *avances de la tecnología* (Arecientes inventos@) --como precisaremos--. Se vislumbra desde aquél entonces una puerta visional del ámbito *iusinformático,* a través de los recientes inventos y como una manifestación más de un único derecho: *The Right to Privacy* o derecho a la intimidad.

Con este proceder no pretendemos desconocer la Aevolución histórica del derecho

---

(22) LOPEZ DIAZ, Elvira. *DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD. Jurisprudencia y Doctrina*. Ed. Dykinson, Madrid, 1996, pág. 197.

(23) Tendremos en cuenta la obra clásico de la literatura jurídica aparecida en el famoso opúsculo de Samuel WARREN y Luois BRANDEIS, denominado: A The Right to Privacy@ (Aprivacy@: Término polémico en su traducción al castellano porque se le ha querido dar diversas connotaciones jurídicas que no tienen en su origen anglosajón, según sea intimidad, privacidad o vida privada, tal como veremos a lo largo de la investigación). El artículo con aquél nombre apareció en la *Harvard Law Review,* Vol. IV., núm. 5, de 15 de diciembre de 1890. *EL DERECHO A LA INTIMIDAD.* Trad. PENDAS, Benigno y BASELGA, Pilar., Ed. Civitas, S.A., 1a ed. Madrid, 1995.

de la intimidad@, relatada a través de las diferentes etapas de la humanidad en forma magistral por *Fariñas Matoni* [24] y fundadas en lo que hoy constituyen los elementos

intrínsecos y extrínsecos de la intimidad, de otras de sus manifestaciones o de derechos autónomos de la persona humana (sentimientos, recuerdos, hogar, vida privada, interioridad humana, daño moral, aspectos corporales o incorporables --v.gr. datos personales--, relaciones familiares, paz y sosiego personal y familiar, honra, domicilio, el honor, la buena imagen, el nombre, etc.), sino delimitar en el tiempo y en el espacio nuestra investigación, tener un referente universal *ab initio* que permita el fundamento teórico-práctico a nuestro planteamiento de igual índole, para desarrollarlo *a posteriori.*

2.1. LA VISION ESTRUCTURALISTA DE LA INTIMIDAD COMO DERECHO.

2.1.1. LOS HECHOS DEL DERECHO.

---

(24) tras recorrer y analizar numerosos textos legales, religiosos, filosóficos e incluso literarios, demuestra los componentes tangibles e intangibles del derecho a la intimidad de las personas ya deambulaba en el ambiente de la humanidad, aunque no con ese término, ni siquiera con el de *privacy* acuñado por la cultura norteamericana, puesto que su cognoscibilidad como concepto con contenido interiorizante del ser humano con proyección al mundo exterior, ni menos como un derecho subjetivo resultaba ajeno a la época histórica y de evolución de la humanidad en cualquier lugar del mundo. En efecto, en la AEdad Antigua@, el Asentimiento de la personalidad@, constituía un valor moral, la conciencia que el hombre occidental tiene del propio ser como un fin en sí mismo, como un centro autónomo de intimidad y de vida. Para los griegos la esencia del hombre era el Aser político@. Para los Romanos, según Von Ihering, el hogar doméstico era importante y cobraba un valor moral. La idea de paz de la casa ha sido reconocida en la inviolabilidad del domicilio en donde era además un lugar santo o sagrado. De ahí el aforismo latino: *ADomus tutissimun cuisque atque receptaculum est@* (Gayo)*:*La casa es para cada cual segurísimo refugio y acogida. En la AEdad Media@. Frente a los Amales@ contra la tranquilidad de las personas debía ser indemnizados, se reconoce en el s.xiv la Aresponsabilidad por agresión y difamación@. En la AEdad Moderna@, en el s. xvi se reglamenta la propiedad literaria. El Ahogar@ cobra mucho más importancia de la que tenía antes. Se plantea la dicotomía de lo Apúblico y lo privado@. En el s.xviii, los ciudadanos intentan definir lo que era Avida pública y lo que no tenía esa calificación. AMientras el hombre se hacía a sí mismo en público, realizaba su naturaleza en el dominio privado, sobre todo experiencias dentro del núcleo familiar@. En las declaraciones de los derechos del hombre formuladas en el s. xviii, Ano contienen mención alguna al derecho a la intimidad@. En 1750, parisinos y londinenses consideraban a sus familias como dominios privados. En la AEdad contemporánea@. La idea moderna sobre los derechos humanos proviene de la oposición entre naturaleza y cultura. Si los sentimientos de un hombre son lesionados, si hacen que se sienta abyecto o humillado, esto constituye una violación a sus derechos naturales. La Glorificación del hogar se alcanzó en Inglaterra (s.xix). Eduard Shils, llamó a la era Victoriana Ala edad de oro de la privacy@ (The golden age of privacy). Establece un relación entre el culto victoriano a la intimidad y la urbanización decimonónica de la vida.@La concepción victoriana de la intimidad fue un medio de defensa contra el código puritano de la época. Incluso, en ciertos aspectos, la intimidad llegó a ser concebida no sólo como un derecho, sino también como un deber: el deber de ocultar ciertas partes del cuerpo@. En esta época, surge en Norteamérica el famoso artículo en la Revista de Derecho de Harvard de Warren y Brandeis (1890). A finales del siglo XIX Engels, se refiere a la familia privada

como la expresión del carácter capitalista. ALa privacidad era el realismo de la expresión interactiva, era una cultura donde los extraños podían inferir el carácter de uno a partir de cómo lucía y cómo vestía. Y aquí esta el punto clave: la creencia de que el secreto es necesario cuando las gentes interactúan plenamente brinda la clave de un barómetro de la angustia psíquica en la sociedad: el deseo de despojarse del sentimiento a fin de no mostrar involuntariamente los sentimientos de los demás.
En 1877, Gareis proclamó el derecho del individuo a organizar su vida como deseare, el derecho al nombre y el derecho al honor. Kohler (1880) defensor de los derechos de la personalidad. Proclamó el derecho a una Aesfera de intimidad@, y en 1907 definió el derecho al secreto. FARIÑAS M., Luis. *EL DERECHO A LA INTIMIDAD*. Ed. Trivium, S.A., Madrid, 1983, págs. 315 a 352.

The Right to Privacy o derecho a la intimidad elevado a rango constitucional en algunos Estados democráticos, como España y Colombia, y en casi todas las legislaciones estatales y universales, es una realidad jurídica que en el mundo occidental comenzó el 15 de diciembre de 1890, con el famoso ensayo jurídico publicado en la *Harvard Law Review* por los abogados Samuel Warren y Louis Brandeis, sobre el derecho que llamaron A*The Right to privacy*@, tras haber sufrido Warren en carne propia la vulneración de éste derecho con la publicación de las actividades personales y sociales mantenidas dentro y fuera de su hogar como repercusión de las escenas que protagonizaba en los sitios públicos y privados con su Avida de lujo y rumbosa@. Actitudes que se agravaban por ser Warren el esposo de la hija de un prestigioso Senador de los Estados Unidos y porque Aatrajo la curiosidad y la chismografía (chismorreo *o Gossip*) de los periódicos en sus crónicas amarillas, hasta el punto de suscitar escándalo@ [24].

2.1.2. PRIMERA PREMISA: ATODO INDIVIDUO DEBE GOZAR DE TOTAL PROTECCIÓN EN SU PERSONA Y EN SUS BIENES@

Los juristas Warren y Brandeis, para estructurar *The Right to privacy* [25], parten del análisis de uno de los fundamentales principios del *Common Law*, que sostiene*: Todo Individuo debe gozar de total protección en su persona y en sus bienes*. Principio revisable como todos los que componen el Common Law por los constantes cambios políticos, sociales y económicos que surgen y se imponen en la misma sociedad que tuvieron origen. En el presente caso, la revisión posibilitó igualmente la redefinición de la naturaleza y extensión de dicha protección.

Los autores para llegar a preguntarse sí en aquella época existía o no un principio de C*ommon Law* que permita invocarse para amparar la privacy (intimidad), analizan los siguientes aspectos: a) La evolución de la concepción jurídicas, efectos y alcances de

---

(24) FROSINI, Vittorio. *INFORMATICA Y DERECHO.* Ed. Temis, Bogotá, 1988, pág.64. Citado en mi trabajo, *LA INFORMATICA Y*... Ob. cit., pág. 27.

(25) Para las glosas y comentarios del Ensayo Warren y Brandeis, seguiremos *ad pedem litterae*, la traducción de Pendás y Baselga. PENDAS, Benigno y BASELGA, Pilar. *EL DERECHO A LA INTIMIDAD. (THE RIGHT TO PRIVACY)*. Ed. Civitas, Madrid, 1995.

los derechos a la vida, a la libertad y a la propiedad que tiene toda persona; b) La Sentencia del Juez *Cooley* (1888), sobre el denominado derecho Aa no ser molestado@[26], cuando se la invaden Alos sagrados recintos de la vida privada y hogareña@, con la toma de fotografías por parte de empresas periodísticas sin el consentimiento de los fotografiados; y c) El escrito de *E.I Godkin*, sobre *The Rights of the Citiezen: To his Reputación* de junio de 1890, en donde evidencia el peligro de una invasión de la intimidad por parte de los periódicos de la época, sobre todo, cuando hacía comentarios sobre la vida personal y familiar de los ciudadanos en detrimento de su reputación, poniéndolas Aen ridículo@ o violando Asu intimidad legal@ [27].

Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos y el Common Law evoluciona para dar cabida a las demandas de la sociedad. Así, los derechos a la vida, a la libertad y la propiedad de las personas, como otros, están evolucionado por dichos cambios y demandas. En efecto, la vida que sólo se protegía de las diferentes formas de violencia, hoy significa el derecho a disfrutar de ella, a no ser molestado. La libertad, ser libre no sometido, a un derecho a la libertad que garantiza un amplio haz de derechos subjetivos; y la propiedad de bienes materiales, hoy abarca tanto a bienes tangibles como intangibles.

En efecto, la evolución significó el reconocimiento legal de las sensaciones, los pensamientos y las emociones humanas, tras reconocer paulatinamente la extensión de la protección contra daños físicos de la mera prohibición a causarlos a la de poner a otro en peligro de sufrirlos (acción de amenazas y, mucho más tarde,

a la protección del individuo contra los ruidos y olores desagradables, contra el polvo y el humo y las vibra- ciones insoportables: el derecho sobre actividades nocivas y molestas tomaba cuerpo).

Las emociones humanas se ampliaron al ámbito de la inmunidad personal más

---

(26) *The right to be let alone*, ha significado para autores como *Vittorio Frossini*, (Ob.cit., pág. 64) --y desde allí *et all*-- el *summun* o la esencia del derecho a la intimidad en sus orígenes. Sin embargo, como vemos en este planteamiento silogístico del trabajo Warren y Brandeis, apenas significa un elemento, importante sí, pero no el único y a manera de primera premisa, de lo que debemos entender integralmente por el derecho a la *privacy* (la intimidad, que es el término que engloba y más fielmente refleja el concepto de privacy): su características, sus limites como derecho no absoluto, sus colisiones y toma de elementos de otros derechos como el del honor o la propiedad intelectual y artística; y en fin, sus mecanismos de reparación o indemnizatoria en caso de daños. Más aún, así se evidencia en el propio ensayo de Warren y Brandeis, se lee: A*La soledad y la intimidad* se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales @. Cfr. PENDAS, B., y BASELGA, P. Ob. cit., págs. 25

(27) PENDAS, B., y BASELGA, P. Ob. cit., págs. 25 y 68

allá del propio cuerpo. Se tomó la buena fama, la protección social (leyes de difamación y libelo). Las relaciones de familia del hombre se convirtieron en parte del concepto legal de su vida, y la pérdida del cariño de la esposa se consideró un daño compensable. En fin, se reconoció los daños y perjuicios por atentado contra los sentimientos de los padres. De la propiedad material surgieron los derechos inmateriales que resultan de ésta, los llamados productos y procesos de la mente, tales como las obras literarias y artísticas, los secretos industriales y las marcas comerciales.

El Juez Cooley denomina derecho *a no ser molestado* (The Right *to be let alone*)[**28**]. Ampara a la persona de Alos recientes inventos@ (fotografía) y los nuevos métodos de hacer negocios. Las fotografías y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: Alo que se susurre en la intimidad, será proclamado a los cuatro vientos@. Desde tiempo atrás se esperaba que un recurso impida la circulación no autorizada de retratos de particulares.

Sin embargo, la invasión en la intimidad, por los periódicos se evidenció tras el escrito de E.I. *Godkin* en Julio de 1890. Un mes atrás, un Tribunal de New York

había reconocido a la prohibición a la circulación de retratos sin el consentimiento del fotografiado (Caso *Marion Manola* Vs. *Stevens* & *Myers*. Junio 1890). Por todo ello, se impone, la necesidad de una protección más amplia de la persona. ALa prensa esta traspasando, en todos los ámbitos, los límites de la propiedad y la decencia. El chismorreo ha dejado de ser ocupación de gente ociosa y depravada, para convertirse en una mercancía, buscada con ahínco e, incluso, con descaro@.

---

(28) En el sentido expuesto por Frossini (nota 26), se sostiene que :@ Samuel D. WARREN y Louis D. BRAN- DEIS, ... exponen, ... las bases técnico-jurídicas de la noción de privacy, configurándolo como un derecho a la soledad, como la facultad de Ato be let alone@ (el derecho a estar solo, o mejor, el derecho a ser dejado tranquilo y en paz), uniéndose en esta expresión --que cobra carta de naturaleza-- a lo llamado, anteriormente en 1888, por el juez COOLEY, AThe Right to be let alone@. Este derecho a no ser molestado significaba, para aquella época, no sólo un factor negativo --como es la posición doctrinaria más difundida actualmente-- , sino también un factor positivo, basada en no dejar circular las fotografías de una persona (La fotografía, era un invento mecánico que invadía abierta y subrepticiamente la vida privada de las personas) sin consentimiento del titular. Estos planteamientos, fueron plasmados judicialmente, como lo asevera la autora citada, al decir que ATres años más tarde de la publicación de este conocido artículo un Tribunal utilizó por primera vez la expresión acuñada por lo dos abogados, Warren y Brandeis, fue el caso MARKS V. JOFFA, fallado por el Tribunal de New York: el demandante, un actor y estudiante de leyes, había visto un retrato suyo publicado en un periódico propiedad del demandado, formando parte de un concurso de popularidad, al que se le oponía personalmente. La sentencia, estimó la demanda y declaró su Aderecho a ser dejado en paz@, basándose en el hecho de que Aningún periódico o institución tiene derecho a usar el nombre o la fotografía de nadie, sin su consentimiento@: Cfr. LOPEZ DIAZ, Elvira. *EL DERECHO AL HONOR Y L DERECHO A LA INTIMIDAD.* Ed. Dykinson, Madrid, 1996, pág. 175

2.1.3. SEGUNDA PREMISA: EXTENSION DEL PRINCIPIO DE LA INVIOLABILIDAD DE LA PERSONA

Ahora bien, el principio invocable para la protección de la *privacy* **[29]**, que no es el empleado para proteger el honor, ni Ael principio que se ha aplicado al amparar estos derechos (los referidos a la propiedad intelectual y artística, en determinados casos de publicación ilegal, los cuales Ano emanan de un contrato, de una buena fe especial, sino que son derechos *erga omnes@*, vale decir, oponibles a todo el mundo: particulares y Estado) no es en realidad el de propiedad privada, por más que esa palabra sea empleada en un sentido amplio y poco usual@ **[30]**. El Principio que no es nuevo en ámbito del Common law, sino extensivo a nuevos hechos (como los aquí comentados), hace parte de un derecho más general el de A*la inviolabilidad de la persona* --del derecho a la propia personalidad--@**[31]** y toma como referentes los siguientes argumentos:

a) No es conveniente ni necesario recurrir a la aplicación analógica del principio empleado por La ley de difamación y libelo [32], para la protección de la privacy, por que ésta abarca solamente los perjuicios causados a la reputación (o el honor), los daños causados al individuo en sus relaciones externas con la comunidad, al hacerle perder la estima con sus conciudadanos, puesto que los derechos reconocidos por aquella ley son, por su naturaleza, más bien materiales que espirituales

b) No existe actualmente --sostenían--, ningún principio bajo el que pueda otor-

---

(29) El Common law, ha Aamparado por siglo y medio la privacy en determinados casos@ aunque en supuestos diferentes; por ello, en los supuestos expuestos por Warren y Brandeis, constituyó, una A aplicación más de la regla vigente@, vale decir, que no se pretendía crear Aningún principio nuevo cuando se hace extensivo este amparo a la apariencia personal, a los dichos, a los hechos y a las relaciones personales domésticas o de otra clase@, sino plantear su reconocimiento a supuestos nuevos. La privacy, en otros supuestos fue utilizada por Lord Cotttenham, en 1820 en el casp Wyatt Vs. Wilson, cuando declaraba, respecto de la actuación de los demandados en aquél caso y sostenía que era Ael derecho a la privacy el que ha sido vulnerado@, en relación con un grabado del Rey Jorge III durante su enfermedad, quien señalaba que Asi alguno de los médicos del anterior Rey hubiera llevado un diario sobre lo que oyó y vio, el tribunal no le hubiera permitido darlo a la imprenta y publicarlo en vida del Rey@. Ibídem. págs. 44 y 59.

(30) AEl significado genuino de la palabra ´propiedad´ en su sentido legal es ´lo que es peculiar y propio de una persona, lo que pertenece exclusivamente a uno´. El principal significado de la palabra de la que se deriva --proprius-- es ´propio de uno. Done on Copyright, pág. 6. Ibídem. 46.

(31) Ibídem, pág. 48.

(32) Pese a esto, las limitaciones al derecho de la intimidad como un derecho no absoluto, según el ensayo Warren y Brandeis, Alas reglas más generales, vienen dadas por las analogías legales que ya fueron desarrolladas en la Ley de difamación y libelo y en la Ley de propiedad intelectual@. PENDAS, B. y BASELGA, P. Ob. cit., pág. 62.

garse una compensación por una ofensa a los sentimientos, aunque ciertamente sea tomada en consideración al determinar la cuantía de la indemnización cuando viene acompañada de lo que se reconoce como una violación de derechos legales.

c) Las infracciones contra el derecho a la propiedad intelectual y artística (el cual constituye uno de Alos ejemplos y aplicaciones al derecho general de la intimidad@[33]), proporciona una reparación a los daños producido a los pensamientos, sentimientos, emociones humanas, en determinados casos.

En efecto, el *Common law* garantiza a cada persona el derecho a decidir hasta que punto pueden ser comunicados a otros pensamientos, sentimientos y emociones. Jamás se podrá forzar a alguien a expresarlos (salvo cuando este comparece como testigo); e incluso, cuando ha elegido expresarlos, retiene por regla general, el poder de fijar los límites de la publicidad que les podrá dar. La existencia de este derecho no depende del medio concreto de expansión utilizado. No importa que sea de palabra o por señas, mediante la pintura, la escritura o la música. La existencia de este derecho no depende tampoco de la naturaleza o valor del pensamiento o de la emoción, ni de la calidad de los medios empleados en su expresión. De igual protección disfrutan una carta intrascendente o unas declaraciones en un periódico que el más valioso poema o ensayo, una chapuza o un pintarrajo que una obra maestra.

Si esto es así, los ensayistas, se preguntan:)Cuál es la naturaleza, el fundamento de este derecho a impedir la publicación de manuscritos u obras de arte?.

1. Sería el del derecho de propiedad, si se toma en cuenta la reproducción de obras literarias y artísticas, pues muchos de los atributos de la propiedad común: son transferibles, tienen un valor, y su publicación o reproducción constituye un modo de materializar ese valor. Pero cuando el valor de la obra no reside en el derecho a obtener las ganancias que se derivan de su publicación, sino en la tranquilidad de espíritu y en

---

(33) Así se sostiene en diversos momentos del ensayo, en particular, previos a la conclusión del planteamiento del principio invocable para la protección de la privacy. Ibídem, pág. 59

el alivio que proporciona el poder impedir su publicación, resulta difícil considerar ese derecho como un derecho de propiedad, en la acepción común del término.

2. Cuando el contenido para el que se solicita el amparo ni siquiera reviste la forma de propiedad intelectual, sino que tiene los atributos de propiedad tangible,

resulta más claramente evidente que este amparo no puede basarse en el derecho a la propiedad literaria y artística en sentido estricto.

Sin embargo, la idea de propiedad ha sido empleada como fundamento para proteger los Amanuscritos inéditos@, y ahora puede tenerse por escrito que el amparo que el *Common Law* proporciona al autor de cualquier escrito es totalmente independiente de su valor pecuniario, de sus méritos intrínsecos, o de cualquier intención de publicarlo, y, desde luego, también enteramente independiente del soporte material, si lo hubiera, o del medio a través del cual el pensamiento o el sentimiento fue expresado [34].

2.1.4. LA CONCLUSION: ATHE RIGHT TO PRIVACY@: EVENTOS.

A esta conclusión, se llega previa el examen de dos conclusiones preliminares: 1. La protección a los pensamientos, sentimientos y emociones humanas, se posibilita mediante el derecho a no ser molestado; y, 2. El derecho a impedir la publicación y reproducción de obras literarias o artísticas, en determinadas circunstancias, sólo es posible, a través derecho a la intimidad como parte del derecho a la inviolabilidad de la persona.

En efecto, vistas las anteriores consideraciones (o premisas) nos llevan -- dicen

---

(34) AAunque los tribunales han afirmado que basaban sus resoluciones en los estrictos fundamentos de la protección a la propiedad, existen sin embargo, indicios de una doctrina más liberal. El caso Prince Albert Vs. Etrange... al hablar de las publicaciones de un individuo que había Aescrito a personas particulares o sobre asuntos personales se refería a ellas como un ejemplo de revelaciones posiblemente ofensivas, al tratarse de asuntos privados y que los tribunales deberían impedir en los casos pertinentes; sin embargo, es difícil concebir cómo, en un caso así, cualquier forma de derecho de propiedad podría ser aplicada a la cuestión, o por qué, dicha publicación debería impedirse como amenaza con exponer a la víctima no sólo del sarcasmo, sino también a la ruina, no debería ser igualmente prohibida cuando amenaza con amargarle la vida. Privar a un hombre de las potenciales ganancias que se obtendrían con la publicación de un catálogo de sus piedras preciosas no puede ser, *per se*, una agravio contra él.... Pero una vez reconocida la intimidad como un derecho protegido legalmente, la intervención de los tribunales no puede depender de la especial naturaleza de los perjuicios causados@. Ibídem., pág. 44 y 45.

los ensayistas *Warren y Brandeis*-- a la conclusión de que la protección otorgada a los pensamientos, sentimientos y emociones manifestadas por escrito o en forma artística, en tanto en cuanto consista en impedir la publicación, no es más que un ejemplo de aplicación del derecho más general del individuo a no ser molestado. Derecho que tiene otros derechos de parecida estructuración y efectos [35].

En consecuencia, el derecho vigente proporciona un principio que puede ser invocado para amparar la intimidad del individuo frente a la invasión de una prensa demasiado pujante, del fotógrafo, *o del poseedor de cualquier otro moderno aparato de grabación o reproducción de imágenes o sonidos* [36]. Protección tanto o igual a la que se deduce de la protección a las emociones y sensaciones expresadas en una composición musical u obra de arte; las palabras dichas, la presentación de una pantomima, como las obras plasmadas por escrito. El hecho de haber sido registrado el pensamiento o la emoción en una forma permanente hace que su identificación sea más fácil, y, por eso, puede tener importancia desde el punto de vista de la prueba, pero carece de significado en cuanto al derecho sustantivo. Así, pues si las resoluciones judiciales sobre los casos de propiedad intelectual y artística, sugieren un derecho general a la intimidad para pensamientos, emociones y sensaciones, éstos deberían disfrutar de igual protección, tanto si se expresan por escrito, o mediante una actuación, una conversación, por actitudes o por un gesto. Aunque obviamente hay que hacer la distinción entre la deliberada expresión de pensamientos y emociones en la literatura u otras composiciones artísticas, y aquella otra, despreocupada y a menudo involuntaria, manifestación de los mismos en las actuaciones de la vida diaria. El amparo, en principio, sólo se refiere a las obras fruto del trabajo consciente.

---

(35) El Right to be let alone de Cooley, es Acomo el derecho a no ser agredido a no ser golpeado, el derecho a no ser encarcelado, el derecho a no ser procesado mediante engaño, a no ser difamado. La cualidad a ser propiedad o posesión es inherente a cada uno de estos derechos, como lo es de cualquiera otros que el derecho reconoce, y, dado que es éste el atributo que distingue a la propiedad, podría considerarse apropiado referirse a estos derechos como una propiedad. Pero obviamente, se parecen poco a lo que, por regla general, se entiende por dicho término. El principio que ampara los escritos personales, y toda otra obra personal, no ya contra el

robo o la apropiación física, sino contra cualquier forma de publicación, no es en realidad el principio de la propiedad privada, sino el de la inviolabilidad de la persona@ . Ibídem., pag. 44.

(36) No imaginaban en aquélla época que tal invasión se iba a sofisticar tanto, hasta llegar a la utilización de medios informáticos, electrónicos y telemáticos, tal como lo comentaremos en la Parte III y IV de esta investigación.

Tras las resoluciones desestimatorias de la distinción que intenta establecerse entre aquellas obras literarias que estaban destinadas a publicarse y aquellas que no, cualquier consideración sobre la cantidad de trabajo necesario, el grado de intencionali- dad, el valor del producto y la intención de publicarse debe ser abandonada, y no se vislumbra una base sobre la que poder sustentar el derecho a impedir la publicación y la reproducción de las llamadas obras literarias y artísticas, como no sea sobre el derecho a la intimidad, en cuanto parte de un derecho más general a la *inviolabilidad de la persona*.

Habría que precisar que los tribunales, en aquellos casos en los que concedió amparo frente a una publicación ilícita, han afirmado su comparecencia, basándose no en la propiedad, o por lo menos no totalmente en ella, sino en el alegado quebrantamiento de un contrato tácito, de la buena fe o de la confianza (así, caso *Abernethy* Vs. *Hutchinson*, Price *Albert* Vs. *Strange*, Tucck Vs. *Priester*, *Pollard* Vs. *Photographic* Co.). Sin embargo, es difícil concebir en base a qué teoría legal se puede acusar de quebrantar un contrato, expreso o tácito, o de violar la buena fe, en la acepción vulgar de este término, al fortuito receptor de una carta que procede a su publicación[37]. Aquí se protege, el derecho a la intimidad por la propiedad del contenido de la carta.

Reconocido el derecho a la intimidad, a título de ejemplo, los ensayistas Warren y Brandeis, exponen los eventos en los cuales se plasma el derecho a la intimidad: a) El derecho de una persona particular a impedir que su retrato circule; b) El derecho a estar protegido de los retratos hechos a mano; c) El derecho a estar protegido de un debate sobre un asunto privado. d) Las relaciones sociales y familiares ante una publicidad despiadada (*My home is my castle)* [38].

---

(37) ASupongamos que se le ha enviado una carta, sin que lo haya solicitado. La abre, y la lee. Con toda seguridad, no ha hecho ningún contrato; no ha aceptado ninguna confianza. Por abrir y leer la carta, no puede

haber contraído ninguna obligación, salvo que lo diga la ley; y, se diga como se diga, esta obligación consiste, únicamente, en respetar el derecho legítimo del remitente, sea cual sea, llámese derecho a la propiedad sobre el contenido de la carta, o llámese derecho a la intimidad@. Aspecto éste que en el derecho actual, tiene regulación expresa en leyes civiles y penales que protegen la intimidad. Ibídem., pág. 57.

(38) Como sostienen al final del ensayo Warren y Brandeis, AEl Common Law ha reconocido siempre que la casa de cada cual es su castillo, inexpugnable a veces, incluso para los propios funcionarios encargados de ejecutar órdenes. Cabe, pues, preguntarse:) Cerrarán los tribunales la entrada principal a la autoridad legítimamente constituida, y abrirán de par en par la puerta trasera a la curiosidad ociosa y lasciva?@ . Ibídem., pág. 73.

2.1.5. LIMITACIONES DEL DERECHO DE LA INTIMIDAD

El derecho a la intimidad, como todo derecho, tiene sus limitaciones que pueden estar en Ala exacta frontera en que la dignidad y la conveniencia del individuo deben ceder ante las exigencias del bienestar general o de la equidad@ [39]. Estas son:

1. *El derecho a la intimidad no impide la publicación de aquello que es de interés público o general* . El objetivo general del derecho, es proteger la intimidad de la vida privada de las personas. Los asuntos por los que una publicación debería ser prohibida pueden describirse como aquellos que hacen referencia a la vida privada, costumbres, hechos y relaciones de un individuo, cuando no tienen una conexión legítima con su adecuación para un cargo público o cuasi público, que busca o para el que es propuesto, y cuando no tienen legítima relación ni nada que ver con algún hecho que haya tenido lugar mientras ocupaba un empleo público o cuasi público; entre otros supuestos [40] .

2. *El derecho a la intimidad no prohíbe la información sobre un tema, aun siendo éste de naturaleza privada, si la publicación se hace en las circunstancias en que, conforme a la ley de difamación y libelo, sería calificada de información privilegiada*. El derecho a la intimidad no se transgrede por hacer público algo ante una autoridad judicial, legislativa, administrativa, así como las noticias sobre algunos de estos procedimientos, en la medida que sean concedidas como un privilegio (Caso Wason Vs. Walters; Smith Vs. Higgins; y, Barrows Vs. Bell). Igualmente, no se prohíbe la publicación que uno hace en cumplimiento de un deber público o privado, ya sea jurídico o moral, o en el manejo de sus propios negocios, y

en asuntos que no conciernen más que a su propio interés (v.gr. Limitación al derecho de impedir la publicación de cartas privadas).

3. *El derecho no otorgaría, probablemente, ninguna reparación por violación*

---

(39) Toma como referente analógico para la determinación de aquellos límites, los que han sido planteados en la ley de la difamación y libelo y en la ley de propiedad intelectual. Muy a pesar , que *ab initio* del ensayo, Warren y Brandeis, proscriben tales analogías, por lo visto, esta tiene una excepción al analizar los límites del derecho a la Aprivacy@. Sobre este punto volveremos en la Parte II de esta investigación. Ibídem., pág. 61-62.
(40) Aclaran los autores, que la relación no es Aexhaustiva@ o taxativa. Ibídem., pág.65

de la intimidad cuando la publicación se haga en forma oral y sin causar daños especiales. Hay que distinguir entre lo que se hace público en forma oral y escrita sobre asuntos privados. El agravio resultante de dicha comunicación oral sería de ordinario tan insignificante que el derecho bien podría, en interés de la libertad de expresión, no considerarlo en forma alguna.

4. *El derecho a la intimidad decae con la publicación de los hechos por el individuo, o con su consentimiento*. Esto es una aplicación de la ley de propiedad literaria y artística.

5. *La veracidad de lo que se publica no supone una defensa*. Se impide es la publicación incorrecta de la vida privada y el que pueda ser descrita.

6. *La ausencia de ´malicia´en quien hace público algo no constituye defensa*. No es causal de excepción al régimen de responsabilidad por daños ocasionados a intimidad, la ausencia de mala fe personal, pues aquí se ampara contra cualquier acción ofensiva, sea punible o no, en sí mismos, los motivos que impulsaron a quien habló o escribió. Esto es lo que ha informado el régimen jurídico de la responsabilidad por daños, en el que alguien es considerado responsable de sus actos intencionados, incluso si son cometidos sin intención malévola (un daño contra la sociedad).

2.1.6. REPARACIONES EN CASO DE VIOLACIÓN DEL DERECHO A LA INTIMIDAD:

Como regla general*: la acción de indemnización por daños*. Incluso en ausencia de daños especiales, puede concederse una compensación substancial por agresión contra los sentimientos, como en la acción de difamación y libelo. En casos especiales: *Un mandato judicial.* La protección de la sociedad, debe venir, principalmente, a través del reconocimiento de los derechos de la persona, uno de los cuales es, la intimidad. Podrá recibir también una protección añadida por el derecho penal [41] .

---

(41) Desde aquélla época se planteaba la posibilidad de proteger a la intimidad a través de la tutela penal y por ello, los ensayistas Warren y Brandeis, citan el trabajo en este sentido de William H.Dunbar, que sancionaban a quien publique en Aun periódico, revista u otra publicación periódica, una declaración sobre la vida privada o los asuntos de otro...@ (Art. 1). Ibídem., pág. 71. En la parte IV de este trabajo tratamos de reflejar la actualidad sobre el particular.

2.2. VISION SOCIOLOGICA O UNIVERSALISTA DE LA INTIMIDAD.

En el presente apartado nos proponemos demostrar la visión universalista del derecho a la intimidad, a partir del análisis de la Declaración Universal de los Derechos del Hombre, de 10 de Diciembre de 1948, adoptada y promulgada por la Asamblea General de las Naciones Unidas en su Resolución 217A (III), en la reunión celebrada en la ciudad de Bogotá, primera en su género, en declarar expresamente a la A*vida privada*@ (oAintimidad@) como derecho objeto-sujeto de protección estatal por parte de los Estados Miembros (entre ellos, España y Colombia). En igual sentido, los diversos Tratados y Acuerdos Internacionales *sobre Derechos Humanos* que siguieron a dicha declaratoria y reconocían y proclamaban expresamente la protección y tutela estatal como la de los mismos particulares del derecho a la intimidad personal, familiar y del menor. Esta visión universalista, ha ido creciendo en forma paulatina y ha evolucionado cada vez más en la sociedad de la primera mitad del siglo XX, teniendo como horizonte el precedente doctrinal del ensayo de *Warren y Brandeis*; los reiteradas decisiones de los Tribunales Americanos sobre la *privacy* que siguieron a éste (basadas en la circulación no autoriza- da de fotografías, del nombre, de la vida pasada o la publicación de imágenes o comenta- rios, opiniones o descripciones periodísticas sin

el consentimiento de su titular [42]); la IV Enmienda a la Constitución de los Estados Unidos de América [43] y la urgencia nece-

---

(42) A título de ejemplo: a) Marks Vs. Joffa (Tribunal de New York, 1893). Un periódico publicó del demandante para una publicidad, sin el consentimiento de Marks (la imagen como parte de la intimidad); b) Robertson Vs. Rocherter Folding Box (New York, 1902). Franklin Mills Co., sin el consentimiento de la joven Abigail Robertson ni la de sus padres, obtuvo, imprimió y vendió e hizo circular litografías y retratos de Abigail (Se reconoció la violación del derecho a la privacy); c) Pavesich Vs. New England Life Insurance Co. (Georgia, 1905). Publicación de foto de la demandante en una publicidad de la empresa de seguros AAtlanta Constitution@; d) Melvin vs. Reid (California, 1931). El productor de cine Reid hizo una película de la Avida pasada de una persona@, sin el consentimiento del titular y aún utilizando su verdadero nombre; e) Philip Shuyler Vs. Ernes Curtis, Alice Donleroy e alt. (New York, 1895). El actor demando a una asociación que tenía la intención de erigir un monumento a su tía difunta. No hubo unanimidad en la decisión del Tribunal, pero el Juez J. Gray, contra la mayoría dijo: Aque el propósito de los demandados había sido la invasión no autorizada del derecho del acto a preservar el nombre y memoria de la difunta frente a los comentarios y la crítica del público@. Ampliamente comentada en: FARIÑAS MATONI, Luis M. *EL DERECHO A LA INTIMIDAD.* Ed. Trivium, S.A. Madrid, 1983, págs. 103 a 143. El Caso OLMTEAD Vs. UNITED STATES (Washington, 1928). Estando como juez Louis Brandeis de la Corte Suprema de los Estados Unidos, afirmó: Alos legisladores de la Constitución norteamericana debieron proteger las creencias, pensamientos, emociones y sensaciones de sus ciudadanos, así como la esfera privada del individuo (idea que más tarde garantizó la Cuarta Enmienda de la Constitución, al proteger la seguridad de sus personas, domicilio y efectos personales frente a cualquier intromisión indebida)@. Cfr. LOPEZ DIAZ, Elvira. *EL DERECHO* ... Ob. cit., pág. 176-177.

(43) Se reconoce el derecho a la privacy en *ALa IV ENMIENDA@,* sostiene: ANo se violará el derecho del pueblo a la seguridad de las personas, hogares, papeles y efectos contra riesgos y detenciones arbitrarias y no menos que hubiese causa probable, apoyada por juramento o afirmación que designe específicamente el lugar que haya de registrarse y las personas u objetos de los cuales haya que apoderarse@.

sidad de proteger y garantizar el derecho a la intimidad en las normas jurídicas de los diferentes Estados del mundo occidental. Necesidades devenidas, entre otras causas, por la sensible vulnerabilidad de aquél derecho, representada por los avances tecnológicos de la información y la comunicación que cada día resultaban más comprometidos en develar la vida particular y pública de las personas (hechos, actos, imágenes, texto, audio), con o sin su consentimiento; así como los que representaba la informática en sus primigenios e incipientes contactos con el derecho [44], tal como lo destaca el abogado norteamericano *Lee Loevinger* en 1949, en lo que denominó *The jurimetric* [45].

Para ello, preliminar y brevemente recordemos uno de los aspectos capitales en el estudio de las ciencias jurídicas, cual es, el referido a las fuentes del derecho, en tanto en cuanto, se ponga en evidencia el origen, el rango o jerarquía y su aplicabilidad en el ámbito de los Estados, como surtidores, creadoras, intérpretes o instrumentos aclaratorios del ordenamiento jurídico interno [46]. Igual importancia, reviste la jerarquía

(44) Alan F. Westin, retrospectivamente observaba los problemas que generaba la naciente informática jurídica, el derecho a la información a que tiene toda persona y el ejercicio de ciertos derechos constitutivos de lo más tarde se llamaría los *derechos de habeas data* (acceso, rectificación y cancelación de información incompleta o indebida). El autor sostenía: AEn las áreas físicas y psicológicas, la ley americana tiene conceptos bien definidos..., pero consideren las dificultades de aplicar normas constitucionales al proceso de información..., la ley americana no tiene ninguna definición... precisa de información... no ha tenido ningún sistema general para tratar el flujo de información que controlan los órganos de gobierno.., excepto algunos ejemplos de datos censales... y las cargas fiscales..., tenemos tradiciones de libre circulación de información... tenemos tradiciones de carácter confidencial y reservas mantenidas en secreto... la ley americana no ha desarrollado procedimientos institucionales para la protección contra la recogida inapropiada de información, almacenamiento de dados inadecuados o falsos, y empleo entre organismos de dicha información... El Act de procedimiento Federal de 1946 aseguraba a los hombres negocio que se enfrenten con sus órganos reguladores federales que ellos conocerían, la información que sobre ellos iba a entrar en los expedientes en ciertos tipos... de juicios orales que ellos tendrían otro oportunidad de presentar otra información para recusar o modificar esta información, y que el expediente sería sometido a revisión... El desarrollo de semejante teoría... fue propuesto... durante... los años cuarenta y ... cincuenta la ley americana queda seriamente afectada por algunos aspectos tecnológicos de los sistemas de información por computador@. WESTIN, Alan F. *SEGURIDADES LEGALES PARA GARANTIZAR LA INTIMIDAD EN UNA SOCIEDAD DE COMPUTADORES 1967*. Citado por FARIÑAS M., Ob. cit. pág. 152-153.

(45) Lee Loevinger en un trabajo titulado: A*Jurimetrics: The next step forward*@, explica como los adelantos tecnológicos, los recursos y procedimientos de manejo de la información al amparo de los computadores u ordenadores y programas (conocidos también como Hardward y Softward), eran válidos para todas la ciencias , y en especial, para las sociales como el derecho. En consecuencia, la jurimetría consistía en una especie de medida del derecho, a través de procedimientos lógicos, racionales y Aautomatizados@ de la información jurídica, en el ámbito financiero y fisca, la cual era aplicable al tratamiento de cualquier cantidad de información jurídica para que le permita al hombre disminuir riesgos de error y aumentar eficacia, rapidez y certeza en el trabajo diario. Más tarde, el procedimiento y métodos utilizados por la jurimetría serían duramente criticados, aunque el fundamento de aquella, aún se utiliza en el tratamiento moderno de la información jurídica (Bases de datos, Thesauros Jurídicos especializados,etc), como veremos en la parte III de este trabajo. Vid. Mi trabajo. *LA CONSTITUCION DE 1991 Y* ... Ob. cit., pág. 109.

(46) No es el momento para hacer un análisis detallado de las fuentes del derecho, pero si destacar, la relevancia e incidencia que tienen en la evolución del derecho, y en particular de los derechos y libertades fundamentales, como la Intimidad, que es ahora nuestro objeto de estudio. Quizá en otro momento, debería hacerse un análisis profundo del tema de las fuentes del derecho, pues el origen y evolución de los derechos humanos (incluidos los fundamentales), se ha debido desde el punto de vista teleológico y normativo, a partir de las llamadas ADeclaraciones Universales de Derechos@ (v.gr. De derechos del Hombre y del Ciudadano de 1789, o la de Derechos del Hombre de 10 de diciembre de 1948, en Bogotá-Colombia), de los Tratados o Convenios Públicos bi o multilaterales, de los pronunciamientos de

y clasificación de aquéllas fuentes del derecho, pero por ahora bástenos solo con decir, que los Tratados Internacionales, en el derecho español se han considerado como fuentes complementarias del derecho, en tanto no hayan sido ratificados por el Estado Español y pasen a formar parte del ordenamiento jurídico, como fuente primaria del derecho, al ser consideradas como leyes de ámbito y aplicación en todo el territorio ibérico [47], no sin antes haber sido publicados oficialmente (art. 96.1 CE).

Las normas relativos a los derechos fundamentales y a las libertades que la Constitución Española reconoce, se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y Acuerdos Internacionales sobre las mismas materias ratificados por España (art. 10.2 CE). Este factor determinante de hermenéutica interpretativa del ordenamiento interno en materia de derechos fundamentales previsto, tanto en la Declaración Universal de Derechos Humanos (que por su naturaleza jurídica no requiere ratificación de los países miembros de la ONU, sino su procedencia, observancia y aplicabilidad), como de los cuerpos normativos internacionales (Tratados y Acuerdos ratificados por España, como p.e., el Convenio Europeo de 1981, en materia de Atratamiento automatizado de datos de carácter personal@), a la luz de la teoría de las fuentes del derecho constituyen una fuente primaria o directa del derecho, si son ratificadas por el Estado Español, previa su publicación oficial en el BOE (Boletín Oficial del Estado) al ser leyes, o bien un conjunto coherente de *principios generales del derecho* [48] sobre determinadas materias, sino no son rati-

---

---CONTINUACION NOTA 46-- los Organismos Judiciales Internacionales (Tribunal de Derechos Humanos, Tribunal de la Haya, Tribunal de la CE, Tribunal Andino, etc.), y en general de los principios generales del derecho generados por los pronunciamientos, decisiones o recomendaciones de los organismos internacionales o comunitarios (UE, ONU, OIT, OEA, OMS, UNESCO, PACTO ANDINO,etc). CONFERENCIAS DE DERECHO ADMINISTRATIVO GENERAL.(Teoría de la ciencia administrativa y organización del Estado). Digitocomputarizadas, Tercer Curso, Facultad de Derecho, Universidad de Nariño, Pasto, 1990, págs. 50 a 63.

(47) Vid. MARTIN MATEO, Ramón. *MANUAL DE DERECHO ADMINISTRATIVO*. Instituto de Admon. Local. Madrid, 1984, págs. 101-107. En igual sentido, ENTRENA CUESTA, Rafael. *CURSO DE DERECHO ADMINISTRATIVO*. Ed. Tecnos, 7a.,ed., 1982, Madrid (Esp.), págs.82-161

(48) Muy a pesar de que MARTIN MATEO, considera que los principios generales del derecho, Ano constituyen fuente en sí mismo, pero sí son aplicables al caso concreto y en un momento histórico determinado. Estos principios rectores intemporales y ahistóricos (conformadores de un Derecho Natural, que no parece posible) parecen no existir en el mundo jurídico actual. El principio de igualdad ante la ley, el principio de equidad de trato, el principio de prohibición de actuaciones arbitrarias, como principios generales del derecho de los cuales se extraen consecuencias jurídicas son invocables directamente ante el Juez para obtener un fallo favorable al caso concreto@. Sin embargo, muchos de estos denominados principios, con el devenir de los tiempos se han ido incorporando en las Constituciones de los Estados (como Colombia y España), hasta tal punto de ir aumentando el catálogo de derechos constitucionales (primera, segunda o tercera generación), y en particular, derechos fundamentales, tales como el derecho a la igualdad, el derecho a la intimidad, el honor, etc., o auténticos *valores constitucionales*, como el de dignidad de la persona, el de libre desarrollo de la personalidad, que en la Constitución Española, constituyen junto a otros derechos fundamentales y el respeto a la ley, en el Afundamento del orden político y de la paz social@ (art 10.1 CE). MARTIN MATEO, R. Ob. cit. pág.50.

ficados y publicados, o en su caso y por su naturaleza jurídica, no necesitan ratificación ni publicación alguna; pero en estos dos últimos casos, con efectos vinculantes de interpretación para los Estados en los casos concretos y ante sus diversos poderes públicos.

En Colombia, la Constitución Política de 1991, es la fuente suprema de fuentes en el derecho interno, por que siendo la *norma de normas* (art.4), Adetermina la estructura básica del Estado, instituye los órganos a través de los cuales se ejerce la autoridad pública, atribuye competencias para dictar normas, ejecutarlas y decidir conforme a ellas las controversias y litigios que se susciten en la sociedad, y al efectuar esto funda el orden jurídico mismo del estado. La Constitución se erige en el marco supremo y último para determinar tanto la pertenencia al orden jurídico como la validez de cualquier norma, regla o decisión que formulen o profieran los órganos por ella instaurados@ (CC. Sent. C-434, Jun.25/1992) [49].

En el sistema de fuentes del derecho público colombiano, la ley constituye la fuente primera y de obligatoria observancia en el ordenamiento jurídico pero derivada de la Constitución (arts. 4 y 230), en tanto que la equidad, la jurisprudencia, los principios generales del derecho y la doctrina son Acriterios auxiliares de la actividad judicial@ (art. 230 *in fine* Id.); vale decir, que sirven como Apautas plausibles de orientación a los tribunales y jueces@, y por tanto, Alas orientaciones así trazadas no son vinculantes sino optativas para los funcionarios judiciales@ (CC.Sent.C-083, Mar.1/1995). Sin embargo, hemos sostenido que las fuentes del derecho no solo se aplican a la función jurisdiccional sino al conjunto de funciones de los poderes públicos en tanto se hallen inmersos en ellas derechos y libertades fundamentales o intereses legítimos sobre los cuales decidir, reconocer, garantizar o tutelar [50].

Los Tratados y Convenios Internacionales Aratificados por el congreso@ (art.93 Ibídem), ingresan al ordenamiento jurídico interno mediante una ley calificada de Aapro-

---

(49) Sentencia de la Corte Constitucional Colombiana (CCC.) AA.VV. *COMPENDIO DE DISCOS DE LEGIS.* Ed. Legis, S.A., Bogotá, 1997.

(50) Mi trabajo, *CONFERENCIAS DE DERECHO ADMINISTRATIVO*...Ob. cit., pág. 63.
batoria de tratados@ que cumple todos los trámites generales y especiales de tales (arts. 160 y ss), y en el caso de los que Areconocen los derechos humanos y que prohíben su limitación en estados de excepción, *prevalecen* en el orden interno@. Prevalencia, que se representa, en la Aprioridad al trámite@ (art.164 Id., reglamentado por Ley 5/1992, art. 217) por parte del Congreso, o Atrámite de urgencia@ (art.163 Id) a petición del Presidente de la República, la veeduría del trámite legislativo por parte del Procurador de la Nación (art.278-4 Id.) y el control constitucional ejercido por la Corte Constitucional, dentro de los seis días siguientes a la sanción de la ley (art.240-10 Id). Trámites y control especiales que no rigen para los Tratados que no involucran derechos humanos (lo cual es discutible), como los de Anaturaleza económica y comercial@ (art.274 Id.) [51].

En igual sentido e interpretación observada en el derecho español, sobre los tratados, Acuerdos o Convenios que ingresan al ordenamiento jurídico interno mediante ley, constituirán fuente primera pero derivada de la Constitución. Caso contrario, configurarán principios generales del derecho para casos concretos, pero como fuentes complementarias del derecho.

2.2.1. Declaración Universal de Derechos del Hombre, de 10 de Diciembre de 1948. Asamblea de la ONU: El Derecho a la intimidad personal y familiar como un ADerecho Fundamental del hombre@.

La Declaración se produjo en un ambiente social, económico, cultural y político *sui generis* en la Colombia de 1948. Sin embargo, haciendo abstracción de aquello, su importancia y efectos socio-jurídicos hacia el futuro fueron decisivos en la normatización o reafirmación de los derechos y libertades fundamentales a nivel interno de los Estados del mundo, pues algunos elevaron a rango constitucional los derechos de la intimidad, de habeas data, de la información, de expresión y del libre desarrollo de la persona-

(51) *A contrario sensu*, que el término Aprevalencia@ se aplica al Avalor preferente de los principios del derecho internacional humanitario en el orden interno@, pues la AConstitución colombiana limita expresamente la competencia de las instancias creadoras y aplicadoras del derecho, en beneficio de la obligatoriedad plena de los principios de derecho internacional humanitario@ (CC. Sent.. C-574, Oct. 22/1992.M.P. Ciro Angarita Barón).

lidad (v.gr. España, Colombia, Portugal, Brasil); otros, expidieron leyes orgánicas, estatutarias o especiales sobre derechos fundamentales, como la intimidad para garantizar y tutelar puntualmente derechos que otrora eran protegidos bajo el amparo de principios, valores o derechos constitucionales más generales (v.gr. derecho al honor, a la honra, a la libertad, la seguridad o la integridad moral).

> *Nadie será objeto de injerencias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataque* (art. 12).

La interdicción de intromisiones en la intimidad de las personas, se toma en la Declaración Universal de Derechos humanos más que un posible concepto primario de la misma, en la traducción literal del término *privacy*, empleado por la jurisprudencia norteamericana, y en particular, en el ensayo socio-jurídico de Warren y Brandeis. Por ello, extraña en la actualidad y en el ámbito iuscivilista que se insista en la diferenciación de aquellos términos, en tanto que diversos cuerpos normativos internacionales sectoriales como los de la Unión Europea (UE), p.e., se utilice indistintamente los términos *vida privada* o *intimidad* en la Directiva 95/46/CE y 97/66/CE, para referirse en esencia, a un derecho inherente a la condición de la persona humana, y por ende, un derecho fundamental garantizado y protegido por el Estado y los mismos particulares.

Las injerencias de toda persona física o jurídica, pública o privada (ANadie@) en la intimidad de otro, se extiende a la de la familia, a su domicilio y a su correspondencia. Se confirma así, la protección no sólo del concepto de intimidad personal sino de la institución socio-jurídica de la familia (o intimidad familiar), la intimidad primigeniamente epistolar, es decir, la correspondencia escrita (pública o privada) y se refuerza expresamente aquello que Warren y Brandeis, citando a los ingleses, denominaron *My home is my* castle (la intimidad domiciliaria). Visiones

conceptuales actuales de la intimidad estas dos últimas (a través de la inviolabilidad de la correspondencia y del domicilio), que preceden al concepto mismo de *the right to privacy,* tanto en la legislación [52], como en las diversas Constituciones del mundo [53].

---

(52) En Colombia, por ejemplo, se reguló la protección del domicilio en el Código Civil de 1887.

(53) En la Constitución de los EE.UU: La IV Enmienda de 1787 (Inviolabilidad de domicilio como de las perso- nas, papeles y efectos); La Constitución de Bélgica de 7 de Febrero de 1831 (El secreto de corresponden- cia es inviolable); La Constitución Argentina de 1 de mayo de 1853 (Inviolabilidad de domicilio); La Constituciones de España de 1869, 1873 y 1876 (Inviolabilidad de correspondencia); y, La Constitución de Colombia de 1886 (Inviolabilidad de correspondencia y domicilio).

El derecho a la intimidad personal y familiar, protegido por la ley contra toda Ainjerencia o ataque@, surge como un Aderecho fundamental del hombre@, cuyo fundamento está: por una parte, en Ala dignidad y el valor de la persona humana y en la igualdad de derechos del hombres y mujeres@; y por otra, en la acción de los Estados en Apromover el progreso social y a elevar el nivel de vida dentro de un concepto más amplio de la libertad@ [54]

Las Constituciones del mundo reconocen explícita e implícitamente el derecho a la intimidad personal y familiar, tal como lo relaciona pormenorizadamente *Fariñas* [55]: la Constitución de la República Democrática Alemana de 7 de Octubre de 1949 (arts.41 y 42); la Constitución Griega de 1 de enero de 1952 (art. 14); la Constitución Portuguesa de 2 de abril de 1976 (art.14); la Constitución Española de 28 de diciembre de 1978; y aunque más recientemente, la Constitución Colombiana de 1991 reconoce expresamente en el art.15 la protección del derecho a la intimidad personal y familiar, ya en la Constitución de 1886, art. 16., se reconocía implícitamente [56].

A título de ejemplo, veamos como las definiciones de la intimidad e inclusión del derecho a Ala vida privada@ en las normas jurídicas para su protección, afloran por doquier. Definiciones que llevan un sello de lo provisional, ya sea por la época, el ámbito, la extensión o limitación del término con el cual se pretendía significar.

En efecto, en 1959, *De Cupis*, tomando los elementos de conceptualización de la *privacy* inmersos en el ensayo Warren y Brandeis y la ampliación institucional vertida

---

(54) Considerando (C.5). Declaración Universal de Derechos Humanos. Texto completo en: AA.VV. *DISCOS COMPACTOS LEGIS.* Ed. Legis S.A., Bogotá, 1997.

(55) FARIÑAS MATONI, Luis. Ob.cit., pág. 251

(56) La Constitución Política de 1886, reconoce el derecho a la intimidad implícitamente, cuando expresa que las Autoridades de la República de Colombia, están instituidas para garantizar y proteger a las personas en Asu vida, bienes y honra@ (art.16). Dicho artículo reconocía el principio del Common law que marcó el punto de partida (Primera Premisa) para la elucubración teórica-práctica de The right to privacy formulado en 1890 por Warren y Brandeis, es decir, el principio de que *Ael individuo debe gozar de total protección en su persona y en sus bienes*@. En el derecho a la libertad de prensa y de opinión (art.42). La Corte Suprema de Justicia, interpretó este artículo sosteniendo que la libertad de opinión Aconsiste en la facultad o poder del individuo de expresar por cualquier medio, publicación, lo que se piensa y cree. Por consiguiente, la palabra, expresión del pensamiento y del contenido de la conciencia es libre, tanto hablada como escrita. La escrita se denomina de imprenta y se manifiesta en el libro, el folleto, el periódico, la revista, el cartel, etc@ (Sent. Marz.31 de 1971). Y, finalmente en el derecho de información contenido en el derecho de petición (art.45). Otros argumentos en mi trabajo, *LA CONSTITUCION DE 1991*... Ob.cit., pág. 25 y ss.

por la Declaración Universal, define la intimidad Acomo aquel modo de ser de la persona que consiste en la exclusión del conocimiento ajeno de cuanto hace referencia a la propia persona o también como la necesidad consistente en la exigencia de aislamiento moral, de no comunicación externa de cuanto concierne a la persona individual@ [57]. Toma el derecho de la intimidad, sólo como el derecho a salvaguardar la ajenidad de la persona (*the right to let alone*), como sujeto individualmente considerado (física como moralmente).

En el ámbito legislativo, la República Federal Alemana, aparece un proyecto de Ley para reordenar la Aprotección a la personalidad y el honor@, reformando así el Código Civil (Junio 10 de 1959), que amplia el concepto de la privacy como el de su protección en base a considerarlo como un derecho de la intimidad personal y familiar. Dicha ley, efectivamente fue redactada bajo la impresión de las indiscreciones de la prensa y la impertinencia de los fotógrafos a su servicio, que ya habían confirmado su evidencia en los estrados judiciales desde 1890. Impresión dubitada por , *De Castro* --según *Fariñas* [58]--, sostenía que la ley contenía Auna poca prudente redacción@, con lo cual se A provocó una violentísima reacción por parte de la prensa alemana y numerosos juristas@ . El proyecto de ley perseguía que Atoda persona que cause un perjuicio a otro en su personalidad está obligado a

reparar el agravio causado@, en los siguientes casos, sin autorización:a) Si profiere o extiende en el público alegaciones concernientes a hechos de la vida privada o familiar de otro; b) Si una persona pública, divulga el contenido confidencial de cartas o notas de naturaleza personal; c) Si una persona publica la fotografía de otro; d) Si una persona, registra las palabras de otro por medios técnicos o las publica, ya sea directamente, ya por medios técnicos; d) Si una persona toma, mediante un dispositivo de escucha o de manera análoga, declaraciones de otro que no le están destinadas o de hechos o acontecimientos relevantes de la vida privada o familiar de otro (arts.15 a 19). Quizá estos dos últimos modos de vulnerar la intimidad con medios tecnológicos, hubiesen sido los antecedentes más próximos para la *Ley de Protección deDatos del Land de Hesse* (Oct.7/70) e incluso de la *Ley Federal*

---

(57) LOPEZ DIAZ, E., Ob. ut supra cit., pág. 188
(58) FARIÑAS M., L., Ob. ut supra cit., pág. 163

Alemana de Protección de Datos (Ene. 27 de 1977), como veremos más adelante.

2.2.1.1. El Convenio para la protección de los Derechos Humanos y las libertades fundamentales de Roma: El derecho a la intimidad personal y familiar es un *derecho autónomo pero no absoluto*.

Los Estados miembros del Consejo de Europa, de aquélla época, tras la Declaratoria Universal de los Derechos Humanos, creyeron conveniente asegurar el reconocimiento y aplicación efectivos de los derechos proclamas por la Asamblea General de las Naciones Unidas el 10 de Diciembre de 1948, a fin de afianzar las bases mismas de la justicia y de la paz en el mundo, y cuyo mantenimiento reposaba esencialmente, de una parte, en un régimen político verdaderamente democrático, y, de otra, en una concepción y respeto comunes de los derechos humanos. Para fortalecer hacia el futuro estos ideales, el Consejo de Europa, acordó la emisión del Convenio de protección de Derechos Humanos y libertades fundamentales, actualmente conocido como *Convenio de Roma de 1950*, y el cual tardíamente fue ratificado por España, mediante instrumento de 26 de Octubre de 1979.

En esencia, el contenido del Convenio es similar a la Declaración de Derechos Humanos, con diferencias puntuales, pero tiene la virtualidad de ser un instrumento jurídico con efectos vinculantes entre los Estados miembros del Consejo de Europa, hoy de la Unión Europea (U). Quizá por ello, actualmente en España, los Tribunales Judiciales en las áreas penal, civil, social (Alaborales@), administrativas, y sobre todo constitucional (TC. Sentencias: Jul. 14/1981; Nov. 15/1982; Jun.6/1994; Feb.23/95; Oct. 25/1995; Dic.11/1995; Mar.3/1996; Jul.9/1996; Mar. 26./1996; Nov. 5/1996), basan sus pronunciamientos en el Convenio de Roma (art.10-2 CE), puesto que los Convenios ratificados por España, tienen efectos jurídicos vinculantes para los poderes públicos y son un factor de interpretación de los derechos humanos (STC Núm. 254/1993, de 20 de Jul.), cuando ingresan al ordenamiento jurídico interno previa publicación en el Boletín Oficial del Estado (BOE art.96-1 CE).

El Convenio, reconoce que *toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás* (art.8).

El Convenio protege el derecho a la intimidad de las personas y de la familia (llámese familia Alegítima e ilegítima@, según el TEDH --Tribunal Europeo de Derechos Humanos-- desde la Sentencia de 13 Jun. 1979 --caso *Marcky*--, en el cual se declaró que *el artículo 8 no distingue entre familia legítima e ilegítima+ v.gr. en el caso *Johnston* --S TEDH 18 Dic. 1986--, tuteló los derechos de una unión conyugal de hecho de más de quince años de convivencia afectiva. Cfr. STC. 184. Nov. 15 de 1990).

De otro lado, establece que el derecho a la intimidad siendo un derecho fundamental y autónomo no es absoluto, lo cual quiere decir, que puede ser limitado o restringido su ejercicio, jamás hacerlo nugatorio, siempre que se den unas causales expresamente previstas. El Convenio, por tanto, proscribe toda injerencia al derecho a la intimidad, salvo que esté prevista: a) en la ley, b) sea necesaria para la seguridad nacional o pública, c) el bienestar económico del país, d) la defensa del orden y la prevención del delito, e) la protección de la salud o de la moral (STC Nov.15/1982, Ala moral pública como límite del derecho de expresión, art.20-4 CE@); y, f) la protección de los derechos y las libertades de los demás.

Estas excepciones a la injerencia e intromisión en el derecho a la intimidad, plantea actualmente uno de los aspectos constitucionales de mayor interés doctrinal y jurisprudencial, cual es el de los límites a los derechos y libertades fundamentales, al reconocérse que éstos no son derechos absolutos en una sociedad democrática y pluralista y tenerse en cuenta que no puede afectarse el contenido esencial (o del núcleo) de los mismos, que los conduzca a desvirturarlo, hacer imposible su ejercicio, o peor aún a eliminarlos. En España, para guardar ese equilibrio del contenido esencial y la aplicabilidad de los límites de los derechos, se acude a la interpretación de los arts. 53-1 y 10 CE, de los que constante y profusamente hablaremos en el transcurso de esta investigación.

2.2.2. Tratados, Acuerdos y Convenios Internacionales que reconocen a la Intimidad como un derecho fundamental e inherente de la dignidad de la persona humana.

Haremos una relación y comentario de estas normas jurídicas internacionales más relevantes en el ámbito americano y Europeo, o en ambos:

2.2.2.1. El A*Pacto Internacional de Derechos Económicos, Sociales y Culturales*@.

Fue adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en la Resolución 2200a (XI) de 16 de diciembre de 1966 [59].

En este documento de la ONU se reconoce el fundamento socio-jurídico y los elementos del derecho a la intimidad, así como la obligación del Estado y los mismos particulares de su respeto y protección.

En efecto, se reconocen los elementos integrales como el fundamento del derecho a la intimidad, paradójicamente sin hacer mención explicita a la vida privada. En efecto, se sostiene que los derechos humanos reconocidos en la Declaración Universal de 1948; entre ellos, la intimidad, se desprenden de Ala dignidad inherente a la persona humana@, por lo tanto, es obligación de los Estados Apromover el respeto universal y efectivo@ de los mismos, y Acomprendiendo que el individuo, por tener deberes respecto de otros individuos y de la comunidad a la que pertenece, está obligado a procurar la vigencia y observancia de A aquéllos derechos (Consideraciones del Pacto).

---

(59) En Colombia se incorporó al ordenamiento jurídico interno mediante la Ley 74 de 1968, de 26 de diciembre.

Los elementos caracterizadores del derecho a la intimidad personal y familiar se hallan tras el reconocimiento de lo siguiente: a) el derecho de toda persona a un nivel adecuado para sí y su familia y basado en el libre consentimiento (art.11-1); b) que la familia es el elemento natural y fundamental de la sociedad, a la que se debe prodigar la más amplia protección y asistencia posible (art.10); c) el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental (art.12), d) que la educación se orienta al pleno desarrollo de la personalidad humana y del sentido de su dignidad (art.13); y, e) el derecho a la vida cultural y al progreso científico.

2.2.2.2. *El Pacto Internacional de Derechos Civiles y políticos de 16 de diciembre de 1966, o también, APacto de New York@.*

El articulado fue adoptado y abierto a firma, ratificación y adhesión por la Asamblea General por medio de la Resolución 2200A (XXI) [60].

Fariñas [61], sostiene que el art. 17 de este documento normativo ONU al reconocer expresamente el derecho a la vida privada, lo hace mediante un contenido textual Acasi idéntico al art. 12 de la Declaración Universal de Derechos del Hombre@. Sin embargo, el marco jurídico en el que esta inmerso es totalmente diferente, porque como veremos junto al derecho de la intimidad se correlacionan otros derechos que influyen directa o indirectamente en su constitución. Además el Pacto Internacional de derechos económicos, sociales y culturales, sirvió de fundamento para el reconocimiento expreso del derecho a la intimidad y otros derechos humanos considerados fundamentales como la vida.

> *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
> *2. Toda persona tiene derecho a la protección de la ley contra injerencias o esos ataques.*

---

(60) En Colombia se incorporó al ordenamiento jurídico interno mediante la Ley 74 de 1968, de 26 de diciembre. En España, se ratificó el Pacto mediante Instrumento de 13 de Abril de 1977.

(61) Ciertamente, las diferencias textuales se centran en la utilización de los términos ilegal y arbitrario para refe- rirse a las injerencias y a los ataques contra la intimidad. Arbitrario, significa contrario a la justicia, la razón o las leyes, dictado sólo por la voluntad o el capricho. Ilegal, contrario a la ley. En el ámbito jurídico resulta más preciso y contundente el término ilegal. FARIÑAS M., L. Ob. cit., pág. 259.

Las diferencias textuales de uno y otro documento jurídico, son nimias frente a las que representa el factor contextual y holístico del derecho a la intimidad, el delineamiento del contenido esencial del derecho [62], las características, sus limites y restricciones y hasta sus colisiones con los demás derechos humanos que se pregonan y tutelan en este Pacto Internacional.

En efecto, todo Estado debe respetar y garantizar a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción los derechos y libertades fundamentales, sin *distinción alguna de raza, color, sexo, idioma,*

religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social (art.2). Aspectos que constituyen la causa y razón de ser de todo derecho humano (en particular, del principio-derecho de igualdad, art.28) y algunos motivos (raza, color, sexo, idioma, religión u origen social) están excluidos de toda causal de excepción y aún en circunstancias excepcionales del Estado (art.4).

El derecho a la intimidad personal y familiar, como derecho fundamental inherente a la persona humana, cuya esencia hunde sus raíces en la dignidad, en el libre desarrollo de la personalidad, igualdad y libertad en una sociedad civil y pluralista se plasma en el Pacto, así: a) En el principio de interdicción en la interpretación que desconoce o reconoce derechos a un grupo o individuo que pretenda quebrantar derechos y libertades de la persona (art.5-1); b) El derecho a la vida es inherente a la persona humana (art.6-1); c) Esta proscrita toda forma de tortura, pena o trato cruel, inhumano o degradante. *Nadie será sometido, sin su consentimiento a experimentos médicos o científicos* (art.7); d) Todo ser humano tiene derecho al reconocimiento de su personalidad jurídica (art.16); e) Toda persona tiene derecho a la libertad de pensamiento, de conciencia y religión (art. 18); f) La familia es el elemento natural y fundamental de la sociedad (art.23); y, g) Todo niño tiene derecho, sin discriminación

---

(62) ***Häberle***, definió el contenido esencial de los derechos como Ael ámbito necesario e irreductible de conducta que el derecho protege, con independencia de las modalidades que asuma el derecho o de las formas en que se manifieste. Es el núcleo básico del derecho fundamental, no susceptible de interpretación o de opinión sometida a la dinámica de coyunturas o ideas políticas@. Citado en la Sentencia de la Corte Constitucional Colombiana (Sent. C.Cons. T-442, Julio 7 de 1992). Texto completo en: WWW. *RDH.GOV.CO* (Base de Datos de la Red Nacional de Derechos Humanos de Colombia). 1998.

alguna, a la protección de su familia como de la sociedad y el Estado (art.24).

Los motivos más comunes y corrientes de colisión del derecho a la intimidad, con otros derechos como los derechos de opinión, expresión e información [**63**], por ejemplo, se patentizan en el ejercicio recíproco de éstos y aquél, y por ello el Pacto reconoce que nadie podrá ser molestado a causa de sus opiniones. Toda persona tiene derecho a la libertad de expresión; *este derecho*

comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras (sean orales, escritas, impresas o artísticas, etc). Este derecho sólo podrá ser restringido expresamente por ley y cuando sea necesario para: 1) Asegurar el respeto a los derechos o a la reputación de los demás, y 2) la protección de la seguridad nacional, el orden público o la salud o la moral públicas (art.19).

Los pronunciamientos de los Tribunales Judiciales sobre A*las injerencias ilegales*@ al derecho de la intimidad, tanto colombianos [64] como españoles [65] han acudido reiteradamente al texto del art. 17 del Pacto de New York, para fundamentar sus pronunciamientos, en aplicación de los tratados internacionales como una de las fuentes del derecho y /o en el factor de hermenéutica interpretativa de los derechos y libertades fundamentales (art. 93 Cons. Pol. y 10-2 CE, respectivamente).

2.2.2.3. *La Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica.*

La Convención se suscribió el 22 de noviembre de 1969, en la conferencia espe-
cializada interamericana de Derechos Humanos [66].

---

(63) En mi trabajo, se abunda sobre el particular. *LA CONSTITUCION*... Ob.cit., pág. 7 y ss.

(64) Así se ha hecho en los pronunciamientos de la Corte Constitucional Colombiana sobre derechos fundamen- tales, en particular del derecho a la intimidad, habeas data, honra, libre desarrollo de la personalidad, a partir de la Constitución de 1991.v.gr. Sentencia T-444, Julio 7 de 1992, T-022 de 1993, Enero 29, T-413/93, de 29 de Sep.,T-454 de 1995, T-696 de 1996, Dic. 5 y T-552 de 1997, de 30 de Oct.

(65) En el Recurso de Casación Núm. 282/1995, el Tribunal Supremo de España, Sala Penal, reitera la jurispru- dencia de la Corporación sobre las injerencias ilegales en la correspondencia, como una forma de vulnerar el derecho a la intimidad (art. 18.3 CE), cuyo basamento se halla, entre otros textos normativos, en el Pacto de New York de 1996, ratificado por España. Sentencia 5-10-1996, Núm. 634/96. Texto completo en. *COMPEDIO DE DISCOS ARANZADI*. Ob. Cit.

(66) En Colombia se aprobó mediante Ley 16 de 1972.

En parecidos términos y contenidos a los anteriores textos normativos internacionales el Pacto de San José, reitera la calidad de derecho inherente a la calidad de la persona humana el que llama Aderecho al respeto de su honra y al

reconocimiento de su dignidad@. El Pacto quiere profundizar más en la protección del derecho a la intimidad (que lo sigue llamando vida privada, como coletilla inseparable de la intimidad) y lo hace yendo a la referencia de dos aspectos del núcleo del derecho como son honra y la dignidad humanas (art. 11). En tal virtud, *nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra injerencias o esos ataques.*

De la esencia del derecho a la intimidad es el derecho que el Pacto denomina ADerecho a la integridad física. 5-1. Toda persona tiene derecho a la que se respete su integridad física, psíquica y moral@. En la actualidad, se ha extendido este aspecto al estudio y análisis de la *visión corporal de la intimidad*, tal como veremos más adelante.

La protección a la Intimidad de la Familia o de la Avida familiar@, tal y como lo hiciera el Convenio de Roma desde 1950, siguiendo en esencia los parámetros de la Declaración Universal de Derechos Humanos, tiene especial relevancia en este Estatuto normativo internacional, por cuanto, se sostiene expresamente Ala protección de la familia@ y sus miembros (en especial del niño art.11), como elemento natural y fundamental de la sociedad, por parte de los particulares y el Estado (art.17).

Desde la *DECLARACION DE LOS DERECHOS DE LOS NIÑOS*, de 20 de Noviembre de 1959 (Resol. 1386), por la Asamblea General de las Naciones Unidas, se ha venido reconociendo la especial protección de estos igualmente especiales miembros de la familia en todas las normas de corte internacional (v.gr. Pacto de New York, Pacto de San José, El Convenio de la Haya de 5 de Octubre de 1961,

sobre competencia de autoridades y la ley aplicable en materia de protección de menores. Ratificado por España, el 29 de Abril de 1984, etc). Sin embargo, fue en las llamadas AReglas mínimas de Beijing-China@, para la Administración de la Justicia de menores, Res. 40/33, de 29 de Nov de 1985 de las Naciones Unidas, en las que se recogió varias recomendaciones formuladas ya en el VI Congreso de la Naciones Unidas para la prevención del delito y tratamiento del delicuente, celebrado en Caracas (Venezuela), en el cual se formuló varios principios básicos dirigidos a dicha protección. En tal virtud, la Asamblea aprobó en Beijin, entre otros aspectos, los siguientes relativos a la protección del derecho a la intimidad de los menores:

> *Para evitar que la publicidad indebida o el proceso de definición perjudiquen a los menores,* ***se respetará en todas las etapas el derecho de los menores a la intimidad****. En principio, no se publicará ninguna información que pueda dar lugar a la individualización de un menor delincuente* (Art.8).

> *Los registros de menores delincuentes serán de carácter estrictamente confidencial y no podrán ser consultados por terceros. Sólo tendrán acceso a dichos archivos las personas que participen directamente en la tramitación de un caso en curso, así como otras personas debidamente autorizadas. Los registros de menores delincuentes no se utilizarán en procesos de adultos relativos a casos subsiguientes en los que esté implicado el mismo delincuente (art. 21)* -- negrillas nuestras --

Posteriormente en la Convención de las Naciones Unidas de noviembre 20 de 1989, sobre Derechos del Niño (Ratificado por España, mediante Instrumento de Nov. 30 de 1990. En Colombia mediante la Ley 72 de 1991), reafirmó la protección y tutela de los Estados miembros de la ONU, del derecho a la intimidad, cuando sostuvo: A*Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni ataques ilegales a su honra y a su reputación. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques*@ (art. 16). Con ello, terminó una etapa amplia y poco fértil de

la doctrina que hasta ese entonces habían negado la titularidad del derecho a la intimidad por parte de los niños.

En Colombia, el Constituyente de 1990, entre otras fuentes normativas próximas para erigir como derecho fundamental en la Constitución la protección del derecho a la intimidad, recogió los parámetros de los Pactos Internacionales anteriores y en especial el del Pacto de San José. En tal virtud, se plasmó en la Constitución de 1991, el derecho a la intimidad de las personas (art. 15, 17, 21, 28 y 74), el derecho a la intimidad familiar (art. 15,17, 28, 33,42, 74) y el derecho a la intimidad de los niños (arts. 15, 21,28, 44 y 50) [67] , y en ningún momento un Aderecho genérico a la intimidad@ (CC. Sent..T-444/1992, de Julio 7. Fundamento Jurídico FJ.1.1.) inexistente doctrinal y legislativamente.

El Pacto de San José, reconoce, de otro lado, el derecho a la libertad de pensamiento y expresión (art.13) y se establece que éste observará el respeto (límite jurídico a otro derecho) del derecho a la intimidad (art.13-2a), y tras proscribir como formas de Apropaganda en favor de la guerra o apología del odio nacional, racial o religioso, que constituyen a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por motivo, inclusive los de raza, color, religión u origen nacional@ (art.13-5), el Pacto reconoce que la información de la persona humana sobre estos aspectos ingresan en el principio de interdicción por cualquier fuente o medio de información.

Junto a estas garantías de la persona, se establece otra de capital importancia en el ejercicio de los derechos de la intimidad, de la información (art.19 de la Declaración Universal de Derechos Humanos; art. 18 del Pacto de New York ; y, art. 13 del Pacto de San José) y el de *habeas data: el derecho a rectificación o respuesta* (art.14). Todos estos Derechos se hallan reconocidos en forma autónoma pero armónicamente regulados

(67) Es pertinente hacer referencia textual a los arts. 17, 28, 33 y 42. El primero, ASe prohíbe la esclavitud...A en sus modernas formas, aún con medios tecnológicos, informáticos y electrónicos. El segundo,@ Toda persona es libre. Nadie puede ser molestado en su persona o familia... ni su domicilio registrado, sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivos previamente definidos en la ley...@ . El tercero, establece: ANadie podrá ser obligado a declarar contra sí mismo o contra su cónyuge, compañero permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil@. El cuarto, ALa familia es el núcleo fundamental de la sociedad... La honra, la dignidad y la *intimidad de la familia son inviolables*...@. Las normas reconocen aspectos importantes que constituyen el contenido esencial del derecho a la intimidad. Respecto de la intimidad de los niños: Art. 44. ASon derechos fundamentales de los niños: la vida, la integridad física, la salud y la seguridad social, la alimentación equilibrada, *su nombre* y nacionalidad, tener una familia...*libre expresión de su opinión.* Serán protegidos contra toda forma de abandono, *violencia* física o *moral, secuestro*, venta, abuso sexual, explotación... Gozarán también de *los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia*...Los derechos de los niños prevalecen sobre los derechos de los demás.@ Cfr. Texto completo: AA.VV. *COMPENDIO DISCOS LEGIS.*. 1997.

a nivel legislativo en los ordenamientos jurídicos internos de Colombia **[68]**, Canadá **[69]**

(68) La Constitución Colombiana de 7 de Julio de 1991, como ya lo había hecho la Constitución de 1886, reconoció el derecho a la información (art.20 y 74) y el derecho de expresión (art. 20 y 73). AEl derecho a la información no es solamente el derecho a informar, sino también el derecho a estar informado, informarse. De ahí la importancias del artículo 74 de la Constitución Nacional, que al consagrar el derecho de acceder a los documentos públicos hace posible el ejercicio del derecho a la información, y de esta manera los demás derechos fundamentales ligados al mismo@, como el *habeas data*, la intimidad, el honor, honra, etc. (CC Sent 0-33, Feb. 8 de 1993). El derecho a la información esta reglamentado en las siguientes normas jurídicas: 1.- Ley 4 de 1913, art.320 (Acceso a documentos públicos); 2.- Ley 74 de 1968, art. 14; 3.- Ley 16 de 1972, art. 13 y 14; 4.- En la Ley 57 de 1985, Julio 5, por la cual se ordenó la publicación y documentos oficiales, conocido en la doctrina como AEstatuto del Derecho a la Información@.Se regula, ente otros aspectos importantes: a) La información reservada: contenido, duración, rechazo --arts. 19 a 21-- ; b) Procedimiento para la consulta de documentos públicos (arts. 22 y ss); y c) Sanciones a los funcionarios que incumplan el contenido de la ley; 5.- El Código Contencioso Administrativo (Decreto 01/1984 y Dec.2400/89). Desarrolla el derecho de petición (art.23 de la C.Pol). Cap.II. El derecho de petición en interés general: peticiones escritas y verbales, término para resolverlas, consecuencias de la desatención de las peticiones, desistimiento (arts.5 a 8). Cap.III. Derecho de petición en interés particular: quiénes pueden hacerlas, requisitos especiales, peticiones incompletas, documentos a información insuficiente, desistimiento, citación de terceros, publicidad, costo de citaciones y publicaciones (arts. 9 a 16). Cap.VI. Del derecho de petición de informaciones: derecho de información, información especial y particular, inaplicabilidad de excepciones, examen de documentos, plazos para decidir sanciones, notificación y recursos a las sanciones, costo de las copias (arts.17 a 24). Cap. V. Del derecho de formulación de consultas: el derecho de petición incluye consultas, atención al público (arts. 25 a 26). El derecho a la información por medios tecnológicos, informáticos y electromagnéticos se rige, por las siguientes normas: 1.- El Dec-ley.131 de 1976 de enero 26, por el cual se dictan normas sobre utilización de sistemas de información y de equipos de información y servicios de procesamiento de datos. Decreto reglamentado por los Dec.1160 de 1976, de junio 7, Res. 2145 de 1976, de Octubre 5. 2.- El Decreto-ley 2328 de 1982, de Agosto 2, por el cual se dictan normas sobre el servicio de transmisión o recepción de información codificada (datos) entre equipos informáticos, es decir, computadores u ordenadores y/o terminales en el territorio nacional. 3.- El Decreto-ley 148 de 1984, de Enero 24, por el cual se dictan normas sobre servicios de transmisión de información codificada (datos) para correspondencia pública. 4.- El Decreto-ley 260 de 1988, de Febrero 5, por el cual se reglamenta el ASistema de Información automatizado en el sector Público@ y las funciones asesoras, consultoras o gestionadoras del DANE (Departamento Nacional de Estadística). Reglamentado por el Dec. 1600 de 1988, por el que se integra una Misión de Ciencia y Tecnología y señala funciones al DANE. 6.- El Reglamento de la Asociación Bancaria y de entidades financieras de Colombia --ASOBANCARIA--, Marzo 23 de 1995, referente al manejo, procesamiento, almacenamiento, uso y transmisión de información económica financiera contenida en las bases de datos de ámbito del sistema del CIFIN --Central de Información de la Asobancaria-- de carácter particular. Las funciones de protección en vía administrativa (Amal llamada gubernativa@, puesto que es viable ante cualquier rama del

poder público y no en forma exclusiva y excluyente de la rama ejecutiva que es lo que sugiere el término Agubernativa@), del derecho de la información la adelanta el Ministerio Público, El Defensor del Pueblo y los Personeros Municipales, pues constituyen una especie de *L´Ombusdman del derecho a la información* o del Comisario para la protección de la información en el derecho Canadiense.

(69) En el Canadá se regula el derecho a la información en forma amplia y compleja en la *Access to information Ac 1980-1983*. En esta se destaca tres aspectos: 1) Protección y tutela del derecho a la información general, personal, familiar o de grupo de cualquier índole: económica, social, cultural, científica, política, etc; 2) Regulación de derechos, deberes y obligaciones de las instituciones gubernamentales, jurisdiccionales y de los mismos particulares con relación al derecho de la información; y 3) Establecimiento del Comisario para la protección de la información (AInformation Commissioner@), con funciones similares en éste ámbito a las que desarrolla el Comisionado para la Intimidad en aquella. La Ley del Derecho de Acceso a la Información en el Canadá (LDAC) Contiene los siguientes aspectos: objetivos, definiciones (Entre otras, ARecord@: dato, información o documento, terceros, deficiencias sensoriables, soportes informáticos o de formato alternativo,etc), derecho de accesso a la información, Información de las entidades públicas, requisitos para ejercitar el derecho de acceso, notificación, emisión de la solicitud, términos, negación de información, comunicaciones, asuntos interinstitucionales, Asuntos internacionales de defensa, Investigaciones, Protección de la información sobre las personas, Información Económica del Estado, *Información Personal* (definición y casos cuando se autoriza la divulgación o autorización Adisclosure@) ,Información de terceros (AThird party information@), Avisos, etc, Exámenes y verficaciones (Atest and audits@), Secreto profesional de los abogados, interdicciones establecidas en otras leyes sobre la información, notificación a terceros, representación de terceros y decisiones, *Recomendaciones del Comisario de la información* (contenido de éstas, recepción de quejas e investigación: quejas escritas, aviso de investigación, aviso a terceros, procedimiento, Secreto de las investigaciones, Poderes del comisionado para la investigación de las vulneraciones del derecho a la información, reportes anuales, revisión de los Tribunales Federales --A Federal Court@--Derechos exigibles, Ejercicio de derechos por el Comisario en defensa del derecho a la información, Aviso a terceros y recursos), procedimientos sumarios, Acceso a los

Australia [70] y España [71]; entre muchos otros Estado del Mundo, muy a pesar, y como veremos en la parte II y III de esta investigación, se sigue creyendo que el derecho a la información es potestativo de los profesionales de los medios de comunicación y no de cualquier persona, la cual, sólo tiene un derecho pasivo a recibir información precisa,

---

--Continuación Nota 69-- documentos, orden de los Tribunales en caso de no autorización a descubrir información, etc. Confidencialidad, Descubrimiento de información autorizada, Información no autorizada, Obstrucciones al ejercicio del derecho de información (actividades ilegales): procedimientos civiles (arts. 1 a 74). Texto completo en inglés y francés, en *WWW.UMONTREAL.EDU.CA* (Database de la Universidad de Montreal, Canadá) 1998.

(70) En Australia, se protege el derecho a la información en la *Freedom of information Act 1982*, complementada por la *Privacy and Data Protection Bill, 1994* -NSW-; Privacy Act, 1988). La ley del derecho a la Libertad de Información, contiene: Parte I. Preliminares (Objetivos, interpretación, etc.). Parte II. Información y publicación de algunos documentos. Parte III. Derecho de Acceso a documentos. Parte IV. Documentos Exceptuados de divulgación, consulta o información (Asuntos de seguridad, defensa o relaciones internacionales, etc). Parte V. Datos e Informaciones personales. Parte VI. Revisión e Investigaciones. Texto completo en inglés, WWW. AUSTLI. EDU.AU (Database de la Universidad de Australia). 1998.

(71) España, se hace referencia expresa a la protección y tutela de la información personal cuando afecta a los de- rechos fundamentales del honor, la propia imagen y la intimidad en la Ley Orgánica 1/1982, de Mayo 5, que regula la protección civil de estos derechos contra las intromisiones ilegítimas; la Ley Orgánica 5/1992, de Octubre 29, sobre regulación del tratamiento automatizado de los datos de carácter personal, o LORTAD. Respecto del derecho de todo ciudadano al acceso a archivos, registros y documentos de las Administraciones Públicas del Estado, se regula en la *LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y PROCEDIMIENTO ADMINISTRATIVO COMUN* (antes LPA)-- Ley 30 de 1992, de Nov.27). El derecho a la libertad de información en el derecho español, se protege y tutela a través de la libertad de expresión (art. 20 CE), donde encuentra abrigo genérico. Quizá por ello, los pronunciamientos del Tribunal Constitucional Español (TC), elucubran sus planteamientos para reconocer el Arecurso amparo@ de las

personas legitimados para incoarlo en dicho argumento. En el Recurso de Amparo 2324 de Enero 1 de 1998, el TRIBUNAL CONSTITUCIONAL, Sala 2, en un reciente caso, que resume la posición del TC, ante el siguiente caso en el cual: AEl recurrente en amparo, trabajador y presidente del comité de empresa en una sociedad concesionaria del transporte público que presentó una denuncia al Ayuntamiento de Oviedo acerca de irregularidades en la prestación del mismo, alega el derecho de cualquier ciudadano de denunciar las irregularidades observadas en el servicio público y que dada su función representativa, ese actuar se incardina dentro de tal función y en ejercicio legítimo de su libertad sindical@. Sostuvo:ALa presencia de este interés (se refiere al interés público en la regular, eficaz y eficiente prestación de servicio público de transporte urbano), por lo demás, viene a dar su máximo sentido al ejercicio de la libertad de expresión, pues es claro que las libertades del art. 20 no son sólo derechos fundamentales de cada ciudadano, sino que significan **el reconocimiento y la garantía de una institución política fundamental, que es la opinión pública libre, indisolublemente ligada con el pluralismo político que es un valor fundamental y un requisito del funcionamiento del Estado democrático+* (STC 20/1990, fundamento jurídico 4.1 a), con cita de las SSTC 6/1981 , 12/1982 , 104/1986 y 159/1986, por todas). Se concluyó: La Vulneración de los derechos fundamentales a la libertad de expresión y a la libertad sindical. Igualmente un reciente AUTO de 23-7-1997, núm. 295/1997. Recurso de Amparo núm. 402/1997 del TRIBUNAL CONSTITUCIONAL, Sala Primera, sostuvo: AUna vez más se nos plantea un supuesto de colisión entre el derecho fundamental a la libertad de información [art. 20.1 d) CE] y el derecho al honor (art. 18.1 CE). En esta ocasión, como en otras muchas, la discusión gravita en torno al concepto de *veracidad+ de la información que la doctrina de este Tribunal ha venido reiteradamente considerando como un límite interno a la libertad de información. (...) 3. Así centrados los términos del debate, no es ocioso recordar que **Cuando la Constitución requiere que la información sea *veraz+ no está privando de protección a las informaciones que puedan resultar erróneas, cuanto estableciendo un específico deber de diligencia sobre el informador, a quien se le puede y debe exigir que lo que transmita como hechos haya sido objeto de previo contraste con datos objetivos, privándose así, de la garantía constitucional a quien, defraudando el derecho de todos a la información, actúe con menosprecio de la veracidad o falsedad de lo comunicado+* (STC 6/1988, fundamento jurídico 5.1). Pero, además, ese deber de diligencia mínima del informador requiere que, a la hora de elaborar la noticia, éste realice una presentación de los hechos que no confunda a sus destinatarios sobre la realidad de lo acaecido, construyendo en realidad una nueva información a partir de la que resulta efectivamente contrastada con las fuentes que se hubiesen utilizado. Máxime **cuando la noticia que se divulga pueda suponer por su propio contenido un descrédito en la consideración de la persona a la que la información se refiere+* (SSTC 240/1992 y 178/1993), o pueda afectar al obligado respeto del derecho de todos a la presunción de inocencia (SSTC 219/1992 y 28/1996). (F.J. 2 y 3). En idéntico sentido: SSTC 204/1997, Nov.11/ y 51/1997, Mar.11.Texto Completo en: *COMPENDIO DE DISCOS COMPACTOS ARANZADI*. Ed. Aranzadi, 1998.
cierta y veraz de quienes ostentan el derecho de expresión.

Sin embargo, cuando el Pacto reconoce el llamado derecho a rectificación y respuesta y definirlo, como aquél que tiene *toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley. En ningún caso la rectificación o la respuesta eximirán de otras responsabilidades legales en que se hubiese incurrido* (art.14) [72], se corrobora la autonomía y la correlación de la existencia de los dos derechos (el derecho a la información como facultad positiva de solicitarla y no sólo a recibirla, y el derecho de expresión), junto al derecho de *habeas data* (acceso a información, rectificación y cancelación).

En éste ambiente de universalización del derecho a la intimidad personal y familiar, de la interiorización del contenido del mismo por parte de los ciudadanos, y del papel que tenía que asumir el Estado, se produce una prolífica legislación en los diferentes ordenamientos internos civiles, penales y administrativos de los Estados del mundo tendentes a proteger, tutelar y garantizar dicho derecho, previos, unos Estados, a elevar a rango constitucional dicho derecho (Portugal en 1976, art. 33, España en 1978, art.18, Alemania, art. 10 y 13)) u otros, a ratificar sus legislaciones preconstitucionales sobre la materia, tal como ocurrió en Colombia, al explicitarse el derecho a la intimidad personal y familiar en la Constitución de 1991, tutelado bajo la visión de Avida privada o íntima@ en el ordenamiento jurídico interno referente a la protección civil (Código Civil de 1887: a) Servidumbre de luz --*intimidad domiciliaria*--, y b) El Daño moral subjetivo

---

(72) Derecho de rectificación o de respuesta, que se extiende no sólo al derecho a la intimidad, sino también cuando el riesgo de vulnerabilidad se presenta en el derecho a la honra y a la reputación (u honor). En efecto, (art. 14-3).

en la responsabilidad extracontractual: *dolor y dignidad humana* [73]) y penal del derecho de intimidad, previsto en los llamados Códigos Departamentales de Policía (v.gr.El del Departamento de Nariño, Ordenanza3 de 1959), y unificada legislativamente en el Código Nacional de Policía (Decretos-leyes 1355-2055/70 y 522/71) [74] y el Có-

---

(73) A la luz de la interpretación constitucional del art. 16 (Protección del Estado de la vida, honra y bienes de las personas) de la Constitución Colombiana de 1886, se ha venido creando jurisprudencia y doctrina iuscivilista sobre protección a la intimidad de las personas, básicamente con dos instituciones jurídicas que desde 1887, están previstas en el Código Civil Colombiano: a) El llamado derecho de vecindad: las servidumbres de luz (Arts.931 y ss.); y b) el no menos delicado como fructífero tema de la AResponsabilidad extracontractual@, de su caracterización, y particularmente de uno de sus elementos más significativo: el daño (arts. 2341 y ss). **A.-** ***Sobre el tema de Servidumbres en general, pero particularmente sobre Alas servidumbres luz@*** que tiene Apor objeto dar luz a un espacio cualquiera, cerrado y techado; pero no se dirige a darle vista sobre el predio vecino, esté cerrado o no. No se puede abrir ventana o tronera de ninguna clase en una pared medianera, sino *con el consentimiento del condueño.* El dueño de una pared no medianera puede abrirlas en ella en el número y de las dimensiones que quiera... La servidumbre de luz está sujeta a las siguientes condiciones: La ventana estará guarnecida de rejas de hierro, y una red de alambre, cuyas mallas tengan tres centímetros de abertura o menos y la parte inferior de la ventana distará del suelo de la ventana a que da luz, tres metros a lo menos@. Nace así en el derecho colombiano el concepto de la Aintimidad domiciliaria@ (AMy home is my castle@ frase férreas y

esquemática por Warren y Brandeis). La intimidad del hogar se protege entre paredes, libres de miradas, comunicación de ruidos, transferencia de olores, etc. En el C.C., se plasma así: i) El que goza de la servidumbre de luz tendrá derecho a impedir que en el suelo vecino se levante una pared que quite la luz. Si la pared medianera llega a ser medianera, cesa la servidumbre legal de luz y sólo tiene cabida la voluntaria, determinada por mutuo consentimiento de ambos dueños; (art. 934 Código Civil--C.C.C--) y, ii) No se puede tener ventanas, balcones, miradores o azoteas, que den vista a las habitaciones, patios o corrales de un previo vecino, cerrado o no, a menos que intervenga una distancia de tres metros. (art.935 C.C.C). Por remisión expresa del art.913 del C.C., los trámites y procedimientos sobre estas servidumbres se traslado a la competencia civil de policía (Inspectores y Alcaldes). Por ello, los Códigos Departamentales y luego el Código Nacional asumieron estas competencias. Vid. Mi trabajo, *LA JURISDICCION CIVIL DE POLICIA.* Tesis para optar el titulo de abogado, Fac. de Derecho, Univ.de Nariño, Pasto, 1983, pág. 33 y ss. **B.-** ***Respecto del derecho a reclamar el Daño Moral*** y su estructuración con base en la dignidad e intimidad de las personas, la Corte Suprema Colombiana, --C.S.J.-- Sala Civil, ha sostenido: 1.- A La doctrina y la jurisprudencia han considerado necesario reservar este derecho (a reclamar el daño moral) a aquellas personas que, por sus estrechas vinculaciones de familia con la víctima del accidente, se hallan en situación de aflicción que les causa la pérdida del cónyuge o de un pariente próximo, de donde se sigue que originándose el emeritado derecho en las relaciones de familia, el demandante del resarcimiento por daños morales quedará legitimado en causa demostrando, con prueba idónea desde luego, la existencia de tales relaciones y que ´el daño moral (que debe) ser cierto para haya lugar a reparación ... quien pretenda ser compensado por el dolor sufrido a raíz de la muerte de un ser querido, tendrá que poner en evidencia, no sólo el quebranto que constituye factor atributivo de la responsabilidad ajena... sino su vinculación con el occiso, *su intimidad con él*, el grado de solidaridad y, por lo mismo, la realidad de su afectación singular y la medida de éste...@ 2.- (C.S.J., Sent. de Nov.24 de 1992). ALa prueba del daño moral, que, cuando proviene del daño a la corporeidad humana, va ínsita en este último@ 3.- (C.S.J., Mar.5 de 1960). 4.- A...el llamado derecho moral subjetivo, por actuar sobre lo más íntimo del ser humano, sus sentimientos, no puede ser justipreciado con exactitud...@ (C.S.J.,Sent. 11 de Junio de 1993. 5.- A ... y los herederos podrían entonces reclamar resarcimiento, pero sólo por derecho propio, en la medida que demuestren quebranto de su individualidad y con él se hiciera presente su padecimiento afectivo o sentimental, habida consideración de los estrechos vínculos que los ataban al muerto (C.S.J., Sent. 20 de Octubre de 1943), justificatiuvos de dicha aflicción y consiguiente derecho (C.S.J.,Sent. 4 de Abril de 1968). Textos completos sentencias en: *DISCOS COMPACTOS LEGIS*. Ed. Legis S.A., Bogotá-Colombia, 1997.

(74) El hecho punible en Colombia se divide en delitos y contravenciones (art. 12 del C.P.), y éstas a su vez se dividen en ordinarias y especiales (art. 12 del Código Nacional de Policía, modificados parcialmente por la Ley 23 de 1991), atendiendo a la gravedad o levedad de la infracción y la sanción, el bien jurídico tutelado y la competencia de las autoridades En el Capitulo VIII. De las contravenciones especiales que afectan a la integridad personal, establece: A El que sin facultad legal averigüe hechos de la vida íntima o privada de otra persona, incurrirá en multa de cincuenta a cinco mil pesos. Si la conducta se realiza por medio de grabación, fotografía o cualquier otro mecanismo subrepticio, la multa se aumentará hasta en la mitad@ (art. 46). AEl que divulgue los hechos a que se refiere el artículo anterior, incurrirá en multa de cincuenta a cinco mil pesos. Si la divulgación se obtiene provecho personal, la multa se aumentará hasta en la mitad. En casos de reincidencia, la pena será de uno a seis meses de arresto@ (art.47). AEl que habiendo tenido conocimiento de un hecho de la vida ajena, la divulgue sin justa causa incurrirá en multa de cincuenta a dos mil pesos. Si divulga el hecho con obtención de provecho personal, la multa aumentará hasta en la mitad@ (art. 48). AEn los casos previstos por los tres artículos anteriores, la acción penal requiere querella de parte@ (art. 49).

digo Penal de 1980 [75].

En el ámbito doctrinal, son ampliamente difundidas y analizadas por los iuscivilistas las definiciones, o mejor conceptualizaciones sobre la intimidad. Destacamos las siguientes:

Para Westin en 1967 [76], define la intimidad como *el derecho de los individuos, grupos o instituciones para determinar por sí mismos, cuando, como y con que*

(75) En el Código Penal de 1980, protege la *intimidad y el habeas* data bajo un bien jurídico tutelado diferente, o bien como derecho fundamental implícito, tal como profundizaremos sobre el tema en la Parte IV de esta investigación. En el Título X, A*De los delitos contra la libertad individual y otras garantías*@, Cap. V, ADelitos contra la violación de secretos y comunicaciones: 1. violación ilícita de comunicaciones (art. 288); 2. violación y empleo de documentos reservados públicos o privados (art. 289); 3. utilización ilícita de equipos transmisores o receptores (incluidos los electromagnéticos: informáticos y/o telemáticos); y, 4. interceptación ilícita de correspondencia oficial. Estos dos últimos previstos en el Dec. Ext. 2266 de 1991, arts. 16 y 18, respectivamente que han sido incorporados a la legislación penal especial en forma permanente. A. *La Fe pública.* En el Título VI, *De los delitos contra la fe pública*, extiende el concepto de documento tradicional (escrito) al concepto de A*documento electrónico*@, cuando incluye en la A*asimilación a documentos...los archivos electromagnéticos*@ (Art. 225 del C.P.Col, conc. Art. 274 C.P.P y 251 C.P.C.). Así debe entenderse que éste concepto se aplicará a los delitos: 1. Falsedad material de empleado oficial en documento público (art. 218); 2. Falsedad ideológica en documento público (art.219); 3. Falsedad material de particular en documento público (art. 220); 4. Falsedad en documento privado (art. 221); 5. Uso de documento público falso (art. 222); 6. Destrucción, supresión y ocultamiento de documento público (art. 223); y, 7. Destrucción, supresión y ocultamiento en documento privado (art. 224). B. *El orden económico social.* En el Título VII, *De los delitos contra el Orden Económico Social*. Se hace referencia expresa a los delitos contra la propiedad industrial, Comercial y Financiera. Estos pueden ser cometidos mediante el uso de elementos informáticos y/o telemáticos. Estos son: 1. Pánico Económico (art. 232); 2. Usurpación de marcas y patentes (236); 3. Uso ilegítimo de patentes (237); 4. Violación de reserva industrial (238). La ley penal especial, principalmente el Dec. 623 de 1993, conocido como A*Estatuto penal del sistema financiero colombiano*@, concede a la Superintendencia Bancaria y de Valores amplias facultades de control, vigilancia, sanción administrativa e información y denuncia ante la Fiscalía General de la Nación sobre actividades delictivas que se presenten en el sector financiero (Bancos, Corporaciones de ahorro y vivienda, corporaciones financieras, sociedades fiduciarias), en todas las gestiones financieras (transferencia, circulación, depósito, ingreso, etc) A*con cualquier forma de dinero u otros bienes*@ (arts. 105 y ss). C. *El patrimonio Económico.* En el Título XIV, *De los Delitos contra el Patrimonio Económico*, se relacionan los siguientes: 1. El Hurto Calificado, cuando se comete con A*llave falsa... o superando seguridades electrónicas u otras semejantes*@ (art.350). Entendiendo por llaves falsas, entre otras, A*las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia*@, tal como lo prevé la legislación penal española (art.239 *in fine*). El C.P.Col., amplia los medios comisivos al preveer la obturación o rupturación de claves o A*password*@ para acceder a la apropiación de bienes. 2. Estafa A*valiéndose de cualquier medio fraudulento...@* como el informático y/o telemático (art.256 *in fine*), configura lo que el C.P. Español denomina A*Estafa informática*@ (art.248), como A*tipo defraudatorio que no comparte la dinámica comisiva de la estafa tradicional y, en consecuencia, ajeno a la elaboración doctrinal y jurisprudencial de los elementos que lo configuran*@. 3. Daño agravado cuando se comete en A*archivos*@ (se entiende manuales o informatizados), art. 371.4. E. *La propiedad intelectual.* Las leyes penales especiales de protección de los programas de computador o A*software*@, la legislación de derechos de autor (Ley 23/32, Ley 44 /94 y D.R.1983 de 1991) y el soporte lógico o A*software*@ (Dec.1360 de Junio 23 de 1989 prevén una gama variopinta de hechos punibles contra el derecho constitucional de la propiedad intelectual (Art.61 Cons. Col.). En el Código Nacional de Policía, reformado por la Ley 23 de 1991, se protege la *intimidad domiciliaria*, al erigir como contravenciones especiales, la violación de habitación ajena (art.1-2), Permanencia ilícita en habitación ajena (art.1-3), Violación de habitación ajena por empleado oficial (art. 1-4), Violación y permanencia ilícita en el lugar de trabajo (art. 1-5). Texto completo en: AA.VV. DISCOS COMPACTOS DE LEGIS. Ed. Legis, S.A., Bogotá-Colombia, 1997.

(76) WESTIN, A.F. *PRIVACY AND FREEDOM.* Atheneum, New York, 1967, p.7. Citado por LOPEZ DIAZ, E. Ob. ut supra cit., pág**.**189.

extensión la información acerca de ellos es comunicada a otros. Define la Aprivacy@ como el *derecho al control de la información referente a uno mismo (A*a Right to control about oneself*@)* .

La conceptualización de la intimidad en Westin abarca, como no podría ser menos, la existencia previa de una causa y razón de cualificar y cuantificarla, cual es

la información que se tiene y puede producir, divulgar o reservarse de una determinada persona o grupo de personas, en la cual se incluye la familia. Recoge el concepto también los elementos característicos de la Aprivacy@, latentes en el ensayo de Warren y Brandeis, que no abandonarán desde el momento que se produjeron hasta la actualidad a cualquier conceptualización de la intimidad: el control de la información de uno mismo o también llamado *autocontrol* de la información (factor positivo de la privacy). Este factor había sido poco conocido por los analistas del ensayo Warren y Brandeis, y sólo se había generalizado el factor negativo de la privacy: *el right to let alone*, que con el transcurso del tiempo ha generado el concepto de la intimidad como un derecho a la soledad, al enclaustramiento, etc. El Factor positivo de la privacy que evidencia Westin, genera la relación armónica que antes comentábamos del derecho a la intimidad, con otros derechos, tales como el de la información, el de habeas data, etc. Por ello, a lo largo de la investigación retenemos ambos factores visionarios de la privacy, pero en especial el positivo por la incardinación con los derechos de la información y habeas data.

Otra conceptualización, que merece reconocimiento en ésta época, es la que adoptaron los Juristas Nórdicos sobre el derecho a la intimidad en la Conferencia de Estocolmo de 1967, retomando las conclusiones vertidas en la Conferencia de Atenas de 1955, en la cual declararon que el derecho a la vida privada Aes inviolable@. Al respecto *López Díaz* [77], relata que la intimidad fue considerada como el Aderecho a ser dejado en paz para vivir su propia vida con el mínimo de injerencias externas@, recogiendo las ideas del Juez Cooley, que sirvieran para delimitar los conceptos de intimidad y vida privada. Cara como inútil labor que perdurará hasta la actualidad sin precisa solución, pues siempre se cae y a veces sin quererlo en la identificación plena, v.gr. El Convenio

---

(77) LOPEZ DIAZ, E. *EL DERECHO AL HONOR*.... Ob.cit., pág. 189.

de Europa de 1981, La LORTAD (LO 5/92, Oct.29), que sólo utiliza el concepto de privacidad en la Exposición de Motivos en tanto que en el texto hace mención a la

intimidad, en el Código Nacional de Policía de Colombia de 1970, etc. El Common Law, por ello utiliza el término genérico de A*privacy*@ para referirse a la vida privada, vida íntima, privacidad o intimidad.

Los Juristas nórdicos, establecieron entonces que el derecho a la intimidad o a la vida privada facultaba al individuo para vivir como él pretende, protegido contra toda injerencia en la vida privada familiar y doméstica, de todo atentado a su integridad física o mental o intelectual, de todo atentado contra su honor o a su reputación, de toda interpretación prejudicial dada a sus palabras o a sus actos, de la divulgación intempestiva de hechos molestos en relación con su vida privada, de la utilización de su nombre, de su intimidad o de su imagen, de toda actividad tendente a espiarla, vigilarle u hostigarle, de la interceptación malévola de sus comunicaciones privadas, escritas u orales, de la divulgación de informaciones comunicadas o recibidas bajo secreto profesional [78] .

---

(78) En la práctica, comprende los casos siguientes: I. El registro de una persona. II. La violación y registro del domicilio o de otros locales. III. Los exámenes médicos, psicológicos y físicos. IV. Las declaraciones molestas, falsas o irrelevantes, referentes a una persona. V. La interceptación de la correspondencia.VI. La captación de los mensajes telefónicas o telegráticos.VII. La utilización de aparatos electrónicos de vigilancia o de otros sistemas de escucha.VIII. La grabación sonara y las tomas de fotografías o películas. IX. La divulgación pública de hechos referentes a la vida privada. XI. La divulgación de informaciones comunicadas o recibidas por consejeros profesionales o dadas a autoridades públicas obligadas al secreto. XII. El acoso de una persona. 41 Este derecho tiene *las siguientes limitaciones:* 1. Los límites necesarios para asegurar el equilibrio entre los intereses del individuo con los de otros individuos, grupos y el Estado. 2. El interés público exige frecuentemente que las autoridades públicas puedan disponer de poderes para inmiscuirse en la esfera privada del individuo más amplios de los que serían aceptables si tal intrusión se realizara por individuos o grupos.3. Tales poderes pueden concederse a una autoridad pública en interés de la seguridad nacional, la seguridad pública, la defensa, el orden y la prevención del crimen, la protección de la salud o de la moral, la protección de los derechos y de las libertades de otro. 4.Los casos de intrusión permitida han de estar definidos con precisión. 5. Respecto a las intrusiones, serán de aplicación las siguientes consideraciones: a) Seguridad nacional, orden público y estado de excepción. I. En tiempo de paz es deseable que se instituya algún tipo de vigilancia o control por autoridad independiente. II. En tiempo de guerra o en caso de situación excepcional, todos los poderes que permitan restringir el derecho al respeto de la vida privada deben ser limitados a los que corresponden estrictamente a los imperativos de la situación y deben cesar al mismo tiempo que el periodo de la guerra o la situación de excepción. III. En casos de catástrofes naturales, las medidas adoptadas deben ser estrictamente proporcionadas a la amenaza producida. b) La prosperidad económica de un país no es un concepto susceptible de una definición precisa. c) La prevención de desórdenes o de actividades delictivas pueden justificar ciertas medidas tomadas en el campo del Derecho penal: I. La investigación de los delitos y descubrimiento de los culpables. II. Perseguir y castigar a los culpables. III. Prevenir las actividades criminales o los desórdenes. d) La protección de la salud puede justificar medidas razonables. 6. La administración de justicia. La medida deberá ser claramente definida.7. Libertad de expresión, información y discusión. La vida privada de las personas públicas debe gozar de inmunidad, salvo si se probare que está íntimamente unida a los acontecimiento público. La libertad de expresión es una de las principales libertades del hombre, de la que dependen otras muchas, que no puede ser restringida por una legitimación especial destinada a proteger la vida privada contra la intrusión de la prensa o de otros medios de comunicación de masas. FARIÑAS MATONI. L. *EL DERECHO A LA INTIMIDAD.* Ob. cit., pág. 312 y 313.

Las conceptualizaciones de la intimidad seguidas a las de *Westin,* concluían en que el derecho a la intimidad, de una parte, es el derecho a ser dejado en paz, a vivir libre de toda injerencia externa por parte de otras personas y, de otra, el derecho a poder controlar la información personal sobre sí mismo (igual *Parker* en 1974 y *Fried* en 1979, *De Miguel* en 1983, *Fariñas* en 1984, *O´Callaghan* y *Pérez Luño* en 1984). Por ello, con diversas matizaciones de estas conclusiones, los doctrinantes, estiman que el derecho a la intimidad es un derecho de la persona (*Battle Sales,1972*), que fomenta y desarrolla la personalidad (*Bajo Fernandez,1980*), inherente a la zona espiritual o interior (*Desantes,1972*), con atributos y poderes (*Albadalejo,1979*), para oponerse a lo público (*Urubayen,1977)* para exigir la no intromisión, indiscreción ajena (*Castán*), vistas, escuchas y captaciones de datos personales (*López Jacoiste,1988*), por cualquier medio tecnológico de la información y la comunicación o TIC y/o informático (*Riascos Gómez, 1990*) y referido a sus relaciones consigo misma o con algunas otras muy cercanas a él, mujer, hijos, padres, algunos amigos, que le rodean en su vida *(Urubayen*) [79], es decir, es un derecho de la persona y de la vida familiar (Constituciones Española, Portuguesa y Colombiana). Este puzle conceptual, no pretende ser un definición perfeccionista de la intimidad, sino demostrar la capacidad de absorción, de porosidad del concepto que permite aumentarlo o disminuirlo según cada autor, parecer, momento histórico, estado de ánimo e incluso de preferencia, inclusión o exclusión de ciertos sectores de la sociedad y ámbito territorial y forma de Estado y Gobierno que pretende proteger, tutelar o garantizarlo. Por estas razones, toda definición de intimidad que se ha planteado y sostenido peca por exceso o por defecto, desvirtúa o lo transforma en otro derecho, tal como sucedió con las posturas opuestas: unas maximalistas y excesivamente patrimonialistas de *William Prosser,* y otras, minimalistas como las de *Blounstein* [80].

En esta época de evolución del derecho a la intimidad, surgen la mayor parte de Leyes protectoras de este derecho en forma autónoma e independiente de otros derechos, aunque no del todo liberadas de la protección conjunta con el derecho al

honor, la propia imagen y el buen nombre. Sin embargo, a partir de la década de los años 70, la irrupción

---

(79) Todos los autores y sus obras, citados íntegramente, a excepción de Riascos Gómez, por LOPEZ DIAZ, E. Ob.cit. págs. 189-196

(80) Ibídem, pág. 205.

de la protección de la protección de la intimidad en todos los ámbitos de la vida cotidiana, la universalización del contenido, se pone en evidencia con mayor fuerza la inusitada aceleración y desarrollo de las nuevas tecnologías de la comunicación y la información (TIC) al abrigo de la informática que tenia la virtualidad de tratar informaciones o datos (*unidades de información codificada por medios electromagnéticos*) de todo tipo. Surge el temor para unos y la visión de evolución para otros del derecho de la intimidad. Comienza a hablarse de la intimidad como un derecho al autocontrol de la información de una persona, el control de la información del concernido, etc. Con este ambiente evolutivo de la intimidad, surge las leyes Suecas, norteamericanas, alemanas, Danesas, Suizas, francesas e Inglesas, que las llaman de Aprotección de la privacy@ , AProtección de los datos@, Arelativa a la informática y los derecho y libertades@, etc., todas ellas producidas entre 1973 a 1984, como veremos más adelante [81].

2.2.2.4. *La Recomendación de la OCDE de 1980 y El Convenio Europeo de Estrasburgo de 1981, sobre Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.*

Estas normas de ámbito internacional europeo, americano, asiático y australiano, son claves en la evolución conceptual de los derecho fundamentales y, en particular del derecho a la intimidad y su visión iusinformática, por ello más adelante haremos comentarios amplios y puntuales sobre aquéllas. Por ahora, veamos brevemente cuales fueron las motivaciones más relevantes previos a su surgimiento y aplicabilidad en 1981,

---

(81) Aparte 4 y ss. Analizamos normas jurídicas prototipo. En Colombia, en 1976, se expiden dos Decretos-leyes y una Resolución reglamentaria del Departamento Administrativo Nacional de Estadística (DANE), por los cuales se A*dictan normas sobre utilización de sistemas de información y de equipos y servicios de procesamiento de datos*@ en el sector público, y que entre otros objetivos tenía, los proteger y garantizar los derechos y deberes de los contratistas con el Estado que utilicen sistemas, equipos y medios computacionales, informáticos, electrónicos o telemáticos. El espíritu que rondaba a aquellas normas no era otro que el de proteger o garantizar derechos de la persona, como la intimidad, que pudieran verse vulnerados en el proceso de contratación administrativa, comercial o civil con el Estado. Aunque no se hubiese planteado en forma explícita , se deduce implícitamente, pues el temor universal por aquella época era el riesgo y la vulnerabilidad que fantasmagóricamente rodada en el ambiente público y privado con la llegada de las nuevas tecnologías de la información y la comunicación apoyadas por la informática y las cuales representaban un filón de mucho cuidado para quebrantar derechos de la persona humana. Los nuevos fenómenos tecnológicos TIC y la informática de labios hacia afuera han representado un gran avance para la humanidad, pero hacia el interior (en el ámbito privsado, y sobre todo público) un leviatán que sigue creciendo desde mediados del siglo y tras su crecimiento sigue produciendo nuevas y variadas formas de temor, riesgo y porosidad.

entre los países miembros del Consejo de Europa.

De los comentarios de *Fariñas* [82], deducimos algunos:

a) Ya en 1968, se había detectado que las técnicas recientemente desarrolladas en la comunicación y la información, la interceptación de las comunicaciones telefónicas y las escuchas clandestinas, representan una amenaza para el derecho y las libertades del individuo, y en particular para el derecho al respeto a la vida privada. En tal virtud, la Asamblea Consultiva del Consejo de Europa, adoptó en la XIX sesión ordinaria la Recomendación No. 509, que evidenciaba esa amenaza y clamaba protección garantista de los Estados.

b) La Conferencia General de la UNESCO, en 1968, declaró que ciertas innovaciones científicas y tecnológicas recientes hacían pesar una amenaza sobre los derechos del hombre en general y especial sobre el derecho a la vida privada.

c) La Conferencia Internacional del Trabajo, en 1970, adoptó en Ginebra la Resolución VII, de 25 de Junio, a la vista de la recomendación de la OIT, por el debido respeto a los derechos sindicales ante el uso cada día más difundido, por parte de los empresarios, de utilización de dispositivos electrónicos de vigilancia para controlar a sus trabajadores.

d) La Asamblea Consultiva del Consejo de Europa sobre *Amass* media@ (luego, multimedia) y derechos humanos, hizo expresa referencia a los bancos de datos (o Aficheros automatizados@, términos éstos que se generalizarían en la Europa ibérica) como Aconcreta amenaza al derecho a la intimidad@, y en tal virtud, deben Arestringirse al mínimo necesario de información indispensable para fines fiscales, programas de pensiones, seguridad social y materias análogas@ (Res. 428 de 23 de Enero de 1970).

e) En Septiembre de 1980, el Comité de Miembros del Consejo de Europa, adop-

---

(82) FARIÑAS MATONI, L., Ob. ut supra cit., pág. 260-261

tó el texto de un AConvenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal@, el estuvo precedido de decisiones, resoluciones, recomendaciones, etc., de la Asamblea Consultiva y del propio Comité de Ministros, así como del grupo de Estados pertenecientes a la Organización y Cooperación para el Desarrollo (OCDE), creada en 1948 y que en 1977, patrocinó un simposio sobre Alas corrientes internacionales de datos y la protección de las libertades individuales@ y en 1980 elevó su propio Recomendación sobre el particular.

f) La OCDE, en Septiembre de 1980, propone la Recomendación de 23 de Enero de 1980, en el ámbito de los países miembros (Estados americanos, europeos, asiáticos y Australia), y en general a la comunidad universal, Apor la cual se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales@, basada en parecidas motivaciones de las del Consejo de Europa.

En la década de los ochenta, se acrecienta la labor legislativa de los Estados por proteger y garantizar los derechos y libertades fundamentales, pero particularmente el derecho a la intimidad, basados en los temores unos reales otros fantasmagóricos que generaban los avances de las nuevas tecnologías TIC y la informática. Esta puntualización sobre el alto riesgo y vulnerabilidad del derecho a la intimidad frente a la irrupción del poder de las tecnologías TIC y la informática, ha sido una de las causas más próximas para que se vuelque las miradas sólo al derecho a la intimidad como único derecho a proteger por los Estados, haciendo abstracción del conjunto de derechos y libertades fundamentales. Nacen así las leyes protectoras del derecho a la intimidad ante las amenazas que surgen de los tratamientos, almacenamiento, utilización y transferencia
de datos de carácter personal, con medios informáticos, electrónicos y telemáticos, o como en el caso del derecho español, adaptan provisionalmente la aplicación de una ley que protege civilmente el derecho a la intimidad, el honor y la propia imagen, para aquellos riesgos potenciales que representa la informática para el pleno ejercicio del derecho a la intimidad (L.O.1/1982, de 5 de Mayo) [83].

La *Privacy Act* Canadiense 1980-83-85, *Ley Islandesa* de 25 de Mayo de 1981, la *Data Protection Act* inglesa de 12 de julio de 1984, La *Privacy Act 1988* de Australia, la Ley Federal Alemana de Protección de datos de 1990 (reformó la Ley de 1977), La Ley portuguesa de 20 Abril de 1991, La LORTAD Española de Oct.29 de 1992 y la *Privacy and Data Protection* 1994 de Australia, conforman el cuadro normativo protector de la década de los ochenta y principios de los noventa, dirigidos inequívocamente a la protección y tutela del derecho a la intimidad.

A título enunciativo veamos el contenido de la *Privacy Act Canadiense* (LAC) [84]. La ley de protección de la intimidad y de los titulares de los datos personales del Canadá contiene 77 artículos y regula, entre otros, los siguientes temas:

a) la LAC como objetivos persigue ampliar la protección a la intimidad ofrecida actualmente por leyes canadienses a los individuos con respecto a la información personal que sobre ellos obtienen las instituciones gubernamentales. A la vez, que se garantiza el derecho de *habeas data* (acceso, rectificación y cancelación) relativa a la información personal de aquellos.

b) Un glosario de términos indispensables para la correcta interpretación de la norma, entre otras, sobre el Comisionado para la protección de la intimidad o APrivacy Commissioner@, El Banco de datos personales o personal information bank o Afichiers@, información personal o Apersonal information@, información financiera, formato alterna-

---

(83) En las Disposiciones transitorias de la mencionada ley se sostiene: @ 1. En tanto no se promulgue la nor- mativa prevista en el art. 18, apartado 4, de la Constitución protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley@. En España así transitoriamente se palió la ausencia de una norma específica que proteja la intimidad del uso de la informática, pero ese no es el gran valor de la norma, sino el que en el derecho ibérico existe una normativa general para la protección civil del derecho a la intimidad (LO 1/82) y una normativa específica para la protección civil y administrativa de la intimidad cuando se halla ante mecanismos informáticos, electrónicos y telemáticos. Este marco protector general y especializado del derecho a la intimidad, ha sido seguido por las leyes canadienses y australianas. El aspecto negativo de estas normas especializadas de protección de la intimidad en forma conductista a ese sólo derecho, es hacer pensar que el uso de la informática sólo puede vulnerar a la intimidad.

(84) ALoi sur la protection des renseignements personnels@, en la versión francesa. Texto completo en WWW. UMONTREAL.EDU.CA. (Base de datos de la Universidad de Montreal de Canadá).

tivo de información Asupport de substitution@ (aplicables a los Adeficientes sensoriales@).

c) Regulación integral del concepto, contenidos y efectos jurídicos de la información considerada personal en todos los ámbitos de la vida (social, política, cultural, investigativa, familiar e intima). Así mismo los ciclos o etapas seguidos en el tratamiento informatizado de la información en la constitución y utilización de los bancos de datos o ficheros. Etapas de recolección, conservación con fines administrativos, Utilización, Registro y descubrimiento (divulgación o revelación) de la información personal. Especial énfasis se hace a la Publicación de índices con información personal.

d) Regulación del habeas data y en forma especial una de sus manifestaciones más caracterizadoras: el derecho de acceso a la información. En tal virtud, dispone que toda persona que ejerza el derecho de acceso, sobre la información personal que está utilizando, ha utilizado, o está disponible su uso con fines administrativo, tendrá derecho además a: a) demandar la corrección de la información personal que le concierne cuando hubiere un error u omisión, o la información fuere incompleta, b) exigir, si fuere del caso, que las mencionadas correcciones reflejen los cambios solicitados; y c) exigir que toda persona u organismo, que haya descubierto información personal para utilizarla con fines administrativos, comunique dentro de los dos primeros años siguientes sobre la corrección o anotación realizada a la información original. Además, tendrá derecho a ser notificado de la corrección o anotación y que el organismo, si se trata de una institución federal, efectúa la corrección o anotación sobre la copia del documento que contiene la información personal del concernido.

e) La información personal concernientes a otro individuo.

f) Regulación amplia de la confidencialidad (secreto), y en especial del secreto Profesional de los abogados con el cliente, Registros Médicos, etc. Igualmente los bancos de datos no consultables, así como sus limitaciones, restricciones y excepciones.

g) El Comisionado para la protección de la Intimidad: Duración, revocación, renovación del mandato, ausencias e incapacidades, Categoría, poderes y funciones, nominación del Comisionado Auxiliar de la Intimidad. Entre las funciones se destaca la de poder iniciar de oficio o a instancia de parte procedimientos para la investigación de las vulneraciones del derecho a la intimidad o a la LAC, los poderes de delegación y subdelegación de funciones para la investigación mencionada (procedimientos breves y sumarios), y si fuere del caso, remitir las por competencia a las autoridades judiciales (civiles, administrativa o penales), si encuentra mérito

para ello. Igualmente rendir informes anuales al Comité Parlamento y otras autoridades gubernamentales. Las decisiones y pronunciamientos del Comisionado son revisables por la Corte Federal.

2.2.2.5. *Las Directivas 95/46/CE y 97/66/CE, del Parlamento y Consejo de Europa, relativos al tratamiento y circulación de datos personales, la transmisión electrónica o telemática de datos y la protección al derecho de la intimidad.*

En el 1995 y 1997, las autoridades legislativas y ejecutivas de la Unión Europea (UE), conscientes de la importancia que tienen actualmente tanto la protección de los derechos y libertades fundamentales, en particular el derecho a la intimidad; como la de viabilizar todo procesamiento, tratamiento, circulación y teletransmisión de los datos personales con miras al mejoramiento de la sociedad y las economías de los Estados Miembros, sin mayores obstáculos jurídicos y tecnológicos TIC e informáticos que los arbitrados en los parámetros normativos mínimos de las Directivas Comunitarias al respecto, las Constituciones Estatales y los ordenamientos jurídicos internos de cada país para la protección de dichos derechos y libertades; y que permiten, entre otros objetivos, no hacer nugatorio el pleno ejercicio de los derechos y libertades fundamentales, ni restringir ni limitarlo a tal punto que lo extingan o esfumen de la vida jurídica. Así se deduce de la lectura del art.1 y Considerandos 8 y 9 Directiva 95/46/CE. Precisamente este marco legislativo comunitario y estatal europeo permiten poner el techo del equilibrio jurídico y social a la libre circulación de datos personales y el respeto, garantía y protección de los derechos, aspectos sobre los cuales ahondaremos en el siguiente aparte.

Las Directivas Comunitarias son interdependientes, como los son los derechos y libertades fundamentales en nuestra actual sociedad. En efecto, cuando en la Directiva 95/46/CE, se reguló todo lo atinente al tratamiento informatizado de datos de carácter personal, por medios informáticos y electrónicos y se

fundamentaron las bases para la transmisión o transferencia de datos de carácter internacional o Aa terceros países@, como prefiere la Directiva. Sin embargo, algunos otros aspectos jurídicos y técnicos, referentes a la teletransmisión de datos y su potencial riesgo y vulnerabilidad sobrevenida a los derechos y libertades fundamentales, y en particular, al derecho a la intimidad fueron tratados específicamente en la Directiva 97/66/CE, para llenar ese evidente vacío previsto en la Directiva de 1995.

El profesor *De la Quadra Salcedo* [85], explica como la Comunidad Europea interviene en la regulación de las telecomunicaciones movida por un propósito de política económica que no es otro que evitar la marginación de la industria europea de las telecomunicaciones, visto que ningún país de la Comunidad representa más del 6% del mercado mundial, en tanto que los Estados Unidos representan un tercio y algo menos Japón. Hoy por hoy, Europa vive un proceso de normativización comunitaria que implica obligatoriedad y efectos jurídicos entre los Estados Miembros, no simples recomendaciones y sugerencias o pautas que era lo habitual en el ámbito comunitario de dos décadas atrás, por eso las Directivas como normas jurídicas al incorporarse al ordenamiento jurídico cumplen esos efectos que en el campo que nos venimos refiriendo permiten proteger unos derechos y libertades fundamentales y potenciar la libre circulación de datos para mejorar el status socio-económico de la UE, en el concierto mundial, reforzado con los procesos de liberalización de las comunicaciones puesto en evidencia hasta ese entonces en la UE (v.gr. Directiva 88/301/CE, liberalización de equipos terminales; Directivas 90/337-388/CEE, liberación de servicios propiamente dichos y de apertura de redes; Resolución Consejo de 22 de Julio de 1993, sobre ampliación sucesiva de la liberalización en telefonía vocal; Directiva 94/46/CE, libre competencia sobre comunicaciones por satélite; Directiva 95/62/CE, sobre aplicación

---

(85) DE LA QUADRA, Tomás. *DERECHO EUROPEO DE LAS TELECOMUNICACIONES.* En: Revista del Consejo General del Poder Judicial. C.G.P.J. No. VI, Escuela Judicial, Centro de Documentación Judicial del Poder Judicial, Madrid, 1997, págs. 47 a 86.

de oferta de red abierta --ONP-- a la telefonía vocal; Directiva 96/2/CE, sobre comunicaciones móviles y personales; y, la Directiva 96/19/CE sobre instauración de la plena competencia en los mercados de telecomunicaciones [86]). En España, el tema de la liberalización de las telecomunicaciones, se ha abordado en el Decreto ley 6 de 1996, de 7 de junio.

En España, la expedición de la Ley 31 de 1987, conocida como *Ley de Ordenación de las Telecomunicaciones* (LOT), LA Ley de Telecomunicaciones por Satélite (Ley 37 de 1995), y el R.D 2.066 de 1996, de 13 de septiembre, por el cual se aprueba el Reglamento Técnico y de prestación del servicio de telecomunicaciones por cable, constituyen la puesta al día en el sector, aunque falta por compatibilizar otros aspectos de las comunicaciones ya previstos en las Directivas Comunitarias desde 1995 hasta la actualidad, pero esencialmente en lo que por ahora nos interesa: protección de derechos y libertades fundamentales y libre circulación de datos personales; es decir, que falta transponer los contenidos de las Directivas 95/46/CE, parcialmente y la Directiva 97/66/CE, integralmente al ordenamiento jurídico interno español.

2.3. LA VISION IUSINFORMATICA DEL DERECHO A LA INTIMIDAD.

El profesor *Morales Prats* [87], al analizar el contenido del derecho a la intimidad, lo hace a través de tres esferas: a) la íntima, b) la relacionada con las libertades políticas; y, c) la relativa a las libertades individuales. El contenido que llama Apreinformático e informático de la privacy@, se inicia con una hipótesis actualmente probada en la doctrina ibérica e internacional, tal y como se ha evidenciado en la visión universalista de la intimidad: la Aprivacy es un derecho política y culturalmente ambiguo@, pero no sólo en el ámbito iuspenalista y constitucional donde surge aquella, sino como lo denuncia *López Díaz*, también lo es, en el ámbito civil y el derecho en general. Por ello, es lógico que exista una gran variedad de criterios, vacíos y contradicciones, tanto en la doctrina como

(86) Directivas ampliamente analizadas por Tomás de la Quadra. Ob. cit., pág. 49 a 86.
(87) MORALES PRATS, Fermín. *LA TUTELA PENAL DE LA INTIMIDAD: PRIVACY E INFORMATICA.* Ed. Destino, Barcelona, 194, pág. 122 y ss.

en la jurisprudencia, a la hora de determinar su contenido del derecho a la intimidad [88], que varía según las épocas históricas; sitios geográficos; ámbitos culturales, sociales, económicos y políticos; legislaciones laxas, prudentes o puritanas; y lo que es aún más evidente a finales del s.xx, según los avances científicos y tecnológicos, especialmente en las ciencias de la información y la comunicación en su entronque con el derecho (ius) y la informática, la electrónica y la telemática.

> A*Meditando sobre la informática y la sociedad se fortalece la convicción de que el equilibrio de las civilizaciones modernas reposa sobre una alquimia difícil: la dosificación entre un ejercicio cada vez más vigoroso, aunque haya que limitarlo, de los poderes soberanos del Estado, y una creciente exuberancia de la sociedad civil. La informática, para bien o para mal, será uno de los principales ingredientes de esta dosificación@* [89]

La telemática, es decir, la imbricación creciente de los ordenadores con las telecomunicaciones, han generado unos Anuevos juegos de poder@, desafíos, expectativas y hasta controversias en esta sociedad informatizada, tal como analizó y visionó en el informe presentado al Presidente Giscard D´Estaing por *Simon Nora y Alain Mic*, el 20 de enero de 1978, en lo que se llamó el A*Informe Nora-Mic@* [90]. Veinte años después, las redes de telecomunicaciones a través de computadores han crecido geométricamente en el mundo, en tanto las normas protectoras o garantístas de los derechos y libertades fundamentales aumentan aritméticamente, poniendo sobre la mesa de equilibrio, nuevas

(88) El Contenido del derecho a la intimidad es variado, amplio y difícil de precisar, cada autor hace una enume- ración y clasificación de supuestos que integran el mismo, lo que no es de extrañar en absoluto, dada la com- plejidad de este derecho y la sujeción del mismo con respecto al tiempo y al espacio. LOPEZ DIAZ, L. Ob. cit., pág.196-197.
(89) Vid. Simón Nora, Inspector General de Finanzas de Francia, de 20 de Enero de 1976, remitido memorial al Presidente Giscard D´Estain.. GARCIA DE PRUNEDA, Paloma. *INFORME NORA-MIC. LA INFORMA- CION DE LA SOCIEDAD.* Ed. Fondo de Cultura Económica, México, Buenos Aires, 1 reeimp., 1982, p. 9.
(90) El Ainforme Nora-Mic@, se realizó a petición del Presidente francés Valery Giscard D´Estain, quien solicitaba (Dic. 20/1976), proponer directrices sociales, jurídicas y técnicas para afrontar Ael desarrollo de las implica- ciones de la informática (considerada) un factor de transformación de la organización

económica y social, y del modo de vida: conviene, pues, --decía-- que nuestra sociedad esté en condiciones de promoverla y a, a la vez, de dominarla, para ponerla al servicio d la democracia y del desarrollo humano@. Los autores prepararon el informe, analizando primero los Adesafíos@: riesgos, posibilidades para el comercio exterior, la situación de la informática en aquella época, los sistemas, redes y equipos instalados y en funcionamiento en las esferas públicas y privadas; pero especialmente los sistemas Atelemáticos@, como generadores de Anuevos juegos de poder@ en todos los ámbitos de la vida política, cultural, educativa, de seguridad social. Una tercera parte de la obra, propone a manera de hipótesis, un interrogante: A)Sociedad Informatizada, sociedad de conflictos culturales?@, y una afirmación: AEl proyecto en un futuro aleatorio: Socializar la información@. ALa informática va a revolucionar nuestras vidas y a va convertirse en un fenómeno de masas.)Hay una política que permita dominar su desarrollo para ponerlo al servicio de todos?. Al modificar los equilibrios del comercio exterior y del empleo, y al poner en tela de juicio numerosas relaciones de poder, la informática permite un crecimiento de nuevo tipo y anuncia una nueva sociedad. Para alcanzarla hay que preservar la independencia de los países respecto de las grandes transnacionales capaces de impedir el desarrollo de una estrategia nacional hacia las telecomunicaciones y los satélites...@ Cfr. NORA, S., y MINC, A., INFORME... Ob. cit., pags. 1-203.

reglas en aquel juego de poder ahora fortalecido por nuevas circunstancias que paradójicamente se fundan en el avance cada vez más penetrante, más sofisticado y difícilmente controlado de las tecnologías TIC y la informática, tal como veremos a lo largo de esta investigación.

El estudio del contenido de los derechos fundamentales, y en particular, en el de la intimidad es de tal variedad como de autores que lo exponen. En efecto, hay tesis con contenidos maximalistas (*Fariñas* [91] y *Novoa Monreal* [92]), otros prudentes (*Prosser*[93], *Frosini* [94]) y otras tantos minimalistas, como la de *Westin* que resume los

---

(91) El Contenido de la intimidad se divide en dos grandes ramas: AI. *En sí mismo, considerado fundamentalmente en cuanto a sí mismo*: 1. Con referencia a su pasado, que es o puede ser evocado en el presente contra su voluntad: a) derecho al olvido, b) derecho a mantener en secreto los recuerdos personales. 2. Con referencia a su presente, en el que es amenazado o atacado: 1) En su propio cuerpo: a)Tomas de sangre, orina, etc., b) Datos sobre su salud, c))Es el aborto una mera cuestión de la vida privada?, d) Narcoanálisis; 2) En aspectos no corporales: a) identidad, b) imagen, c) Datos personales, d) ser seguido u observado, e) objetos personales, f) placeres. 3. Con referencia a su futuro en cuanto planeado en el presente, potencialmente amenazado por ataques actuales: a) Descubrimiento de planes o proyectos del futuro. II. En sí mismo, considerado fundamentalmente respecto de los otros: 1. Los otros en cuanto colectivo: a) El Estado, en su doble papel de garante y amenaza de la intimidad; b) Personal (garante en cuanto emisor de normas protectoras, amenaza en cuanto compilador de otros datos personales, c) la sociedad y su interés en ser informada. 2. Los otros en cuanto personas concretas. 3. La intimidad ajena como límite y condicionante de la propia (el problema de la divulgación unilateral de un secreto compartido sin el consentimiento de la otra persona: a) la intimidad propia compartida: relaciones familiares (hogar, vida conyugal), relaciones cuasifamiliares (aventuras amorosas, amistades, comunicaciones y cartas), relaciones profesionales (vida profesional, secreto de los negocios); b) La intimidad propia amenazada por los otros: individuos concretos (parientes, vecinos, amigos, compañeros de trabajo, superiores, subordinados, extraños), sociedades, entidades o institucionales especializadas ad hoc (detectives, agencias de información o matrimoniales, otras entidades), El Estado (como administración y/o mediante sus funcionarios que cumplen o extralimitan sus funciones). FARIÑAS MATONI, L. Ob.cit., pág. 314 y ss.

(92) ALa vida privada esta compuesta por: 1. Ideas y creencias religiosas, filosóficas, mágicas y políticas que el individuo desee sustraer al condicionamiento ajeno. 2. Aspectos concernientes a la vida amorosa

y sexual. 3 Aspectos, no conocidos por extraños, de la vida familiar, especialmente, los de índole embarazosa para el individuo o para el grupo. 4. Defectos o anomalías físicas o psíquicas no ostensibles. 5. Comportamiento del sujeto que no es conocido de los extraños y que, de ser conocido, originaria críticas o desmejoraría la apreciación que estos hacen de aquel. 6. Afecciones de la salud, cuyo cumplimiento menoscabe el juicio para fines sociales o profesionales formulan los demás acerca del sujeto. 7. Contenido de comunicaciones escritas u orales de tipo personal, esto es dirigidas únicamente para el conocimiento de una o más personas determinadas. 8. La vida pasada del sujeto, en cuanto puede ser motivo de bochorno para este (derecho al olvido). 9. Orígenes familiares que lastimen la posición social y en igual caso, cuestiones concernientes a la filiación y a los actos del estado civil. 10. El cumplimiento de las funciones fisiológicas de excreción, hechos o actos relativos al propio cuerpo que son tenidos por repugnables o socialmente inaceptables (ruidos corporales, etc). 11. Momentos penosos o de extremo abatimiento. 12. En general, todo dato, hecho o actividad personal no conocidos por otros, cuyo conocimiento por terceros produzca turbación moral o psíquica al afectado (desnudez, etc.)@. Citado por LOPEZ DIAZ, E., Ob.cit. pág. 207.

(93) William Prosser (1964). Agresiones a la privacy: 1. La intromisión en la soledad física que cada persona se ha reservado. 2. La divulgación pública de hechos privados.3. La presentación al público de circunstancias personales bajo una falsa apariencia o divulgación de hechos que suscitan una falsa imagen para el interesado a los ojos de la opinión pública. 4. La apropiación indebida, en sentido amplio, de lo que pertenece a nuestro ámbito personal@ Citado por LOPEZ DIAZ., E. Ob. cit. pág. 200

(94) Vittorio Frossini. 1. Soledad: que supone la imposibilidad física de contactos materiales. 2. La intimidad: sin hallarse aislado el individuo se encuadra en un grupo reducido (ámbito familiar). 3. El anonimato: que mantiene la libertad para identificaciones individuales. 4. La reserva: creación de una barrera psicológica frente a intrusiones no deseadas@. Citado por LOPEZ DIAZ, E. Ob.cit., pág. 199.

estadios de la privacy (Soledad, relaciones íntimas, anonimato y reserva), en A*el derecho de los individuos, grupos o instituciones de determinar por ellos mismos, cómo y cuanta información acerca de sí es comunicada a los otros@.*

En su justo medio, el derecho español, como no podía ser menos, debido a la complejidad para determinar el contenido del derecho a la intimidad, según la doctrina y legislación universal, ha constitucionalizado dicha situación en el art.18 de la Constitución Española de 1978, al presentar diversos supuestos en los que éste se encuentra, antes que una definición de la intimidad o de elementos que la caracterizan o develen su contenido único y hermético. Esto revela que existe en la Apráctica una gama variada de aspectos o facetas de la misma, aparentemente sin relación entre sí, pero que constituyen manifestaciones de un único derecho@, tal como lo sostiene *Vidal Martínez* **[95]**. Entre esas facetas están: a) la inviolabilidad de domicilio, b) El derecho al secreto (en comunicaciones, documental, profesional -- abogados, notarial, médico, religioso, periodístico, bancario --, y c) *Intimidad versus tratamiento informatizado de datos* **[96]**, vale decir, la visión iusinformática del derecho a la intimidad.

Cada una de estas facetas ha dado lugar a estudios autónomos y especializados, tal es el caso de la intimidad de la corporeidad humana de palpitante

actualidad (v.gr. *Gil Hernández, Cano i Arteseros* [97]); vale decir, *la visión en la corporeidad de la intimidad* per se no física, pero si ligada estrechamente a ella, pues hace parte de la intimidad personal de todo ser humano, de principio inmune, frente a toda intromisión no autorizada por la ley, una orden judicial, o por voluntad o consentimiento de

---

(95) Citado por LOPEZ DIAZ, Ob. cit., pág. 210
(96) Ibídem., pág. 210-257.
(97) Este derecho a la intimidad corporal inherente a la diginidad y personalidad del ser humano, en cuanto a su ámbito no sólo conceptual sino geográfico entonces, @esta determinada en cada sociedad y en cada momento histórico@ (STC Núm. 171/1990, de 5 de noviembre) de su evolución del hombre, puesto que es de la esencia de las personas como el derecho dicha transformaciones y condicionamientos. Hasta hace unas dos décadas era impensable una controversia judicial, e incluso social, la vulneración de la intimidad, además de otros derechos (v.gr. Libre desarrollo de la personalidad, art.16 Cons.Col.) y valores constitucionales (dignidad humana), mediante las intervenciones corporales, sin el consentimiento de la persona o de sus representantes legales en el caso de los niños (Corte Constitucional Colombiana (CC), Sent. T-477/1995). GIL HERNANDEZ, Angel. *PROTECCION DE LA INTIMIDAD CORPORAL: ASPECTOS PENALE S Y PROCESALES.* Revista General de Derecho. Jul-Ago. Núm. 622-623, Valencia, 1996, págs.7949 y ss. CANO U ARTESEROS, Silvia. LA INTIMITAT CORPORAL SEGONS LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL. En: Revista de Catalunyz No. 4, Ed. Jurídica Barcelona, 1995, pág. 127 y ss. Vid., Sentencia de la Corte Constitucional, en *WWW. RDH.GOV. CO*. 1998.

la persona concernida, por ejemplo, A frente a toda indagación o pesquisa que sobre el cuerpo quisiera imponerse... cuyo sentimiento de pudor queda así protegido por el ordenamiento, en tanto responda a estimaciones y criterios arraigados en la cultura de la comunidad@ (STC Núm. 37/89, de 15 de febrero).

La Constitución española con respecto a la visión iusinformática de la intimidad, que *Lopez Díaz*, considera una manifestación o faceta más de ese único derecho llamado de la intimidad, se relaciona en el art. 18-4 CE, cuando sostiene: A*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*@, indicando con esto, que la informática como tecnología que procesa lógica, ordenada y concatenadamente cualquier cantidad o clase de información con medios, soportes, aplicaciones informáticas, electrónicas y telemáticas, esta instituida en la constitución para garantizar el efectivo ejercicio del conjunto de derechos y libertades fundamentales y no sólo de los derechos a la intimidad y al honor, como pudiera pensarse. En España, como en el resto de países del mundo, las legislaciones

han dado esta impresión, al reglamentar el Auso de la informática@ sólo referido al derecho de la intimidad, tal como precisaremos más adelante.

La informática en su entronque con el derecho forma la *iusinformática,* --tal como se evidencia en la Constitución de España, la Portuguesa de 1976 (art.35) y la Colombiana de 1991(art.15)-- la cual, a través de normas Aprotectoras de los datos@ (caso alemán, sueco, danés, español, etc), de la protección de la Aprivacy@ (norteamericana 1974, Canadiense 1988, y Australiana 1994) o de la protección del Aderecho a la libertad de información@ (AAcces Information Act@ Canadiense, la AFreedom of information@ Australiana, o las normas del Estatuto de la información Colombiano) va a regular todo lo atinente al empleo, uso, utilización, conservación, transmisión de los medios informáticos, electrónicos y telemáticos, pero sobre todo, los supuestos expresos de limitación a su uso por cualquier persona (natural, jurídica, pública o privada), sin que ello signifique su restricción sin mínimos, o peor aún su desaparecimiento o verse desvirtuado .

Frossini, tras el análisis del ensayo de *Warren y Brandeis*, consideró que la libertad de la persona referidas al control de la información de sí mismo por sistemas computacionales constituía una especie de A*Libertad informática*@ [98]. Esta tesis hizo curso en el derecho español en términos de *Pérez Luño* y *Morales Prats* [99], hasta el punto que hoy día se identifica la visión iusinformática de la intimidad con la Alibertad informática@, también llamada Aintimidad informática@ [100] o A*derecho de autodeterminación informativa*@ (basado en el derecho fundamental al Libre desarrollo de la personalidad, que en Alemania y Colombia, sí son derechos autónomos. Art.16 Cons.Pol.) [101], pero estos tres últimos como derechos fundamentales autónomos. A pesar de lo variopinto de las nominaciones, en nuestro criterio, el derecho a la intimidad sigue siendo uno solo y múltiples sus manifestaciones, facetas o visiones, todas variadas en la medida que fundamentan su estructura, sin perder identidad y autonomía, en las diferentes fuentes doctrinales, legislativas y jurisprudenciales y/o en la concatenación con otros derechos, valores o principios constitucionales de los cuales toman sus elementos característicos, sus

facultades y relevancias. En nuestro caso, este ha sido el procedimiento metodológico para desentrañar la visión iusinformática de la intimidad, que reconoce la existencia de la intimidad como derecho fundamental autónomo y la visión iusinformática o iustecnológica, como una de sus últimas facetas devenidas de las nuevas tecnologías TIC y la informática. De esta forma no hablamos de un derecho

---

(98) FROSSINI, Vittorio. *LA PROTECCION DE LA INTIMIDAD: DE LA LIBERTAD INFORMATICAM AL BIEN JURIDICO INFORMATICO.* En: Revista Derecho y Tecnología Informática. No.3 Ed. Temis, Bogotá, 1990, pág.19.

(99) @Debe insistirse en que el derecho fundamental a la libertad informática no se limita a la protección de los datos en el momento de su transmisión o utilización, sino que nace y puede ejercitarse desde el mismo momento en que los datos son almacenados. Por ello, se confiere al titular un *control preventivo* de los datos almacenados@. PEREZ LUÑO, A. *DERECHOS HUMANOS, ESTADO DE DERECHO Y CONSTITUCION.* Cap. 10. Intimidad e informática en la Constitución. Ed. Tecnos, Madrid, 1984, pág.370 y ss. MORALES PRATS, sigue las posturas del profesor Pérez Luño en el reconocimiento de la libertad informática como derecho fundamental autónomo, en las obras ut supra cit.

(100) El autor reconoce la calidad de derecho fundamental autónomo del derecho a la libertad informática que él denomina Aintimidad informática@ . SARDINA VENTOSA, Francisco. *EL DERECHO A LA INTIMIDAD INFORMATICA Y EL TRATAMIENTO DE DATOS PERSONALES PARA LA PREVENCION DEL FRAUDE.* En: Revista Actualidad informática Aranzadi. Ed. Aranzadi, S.A. No. 25 de octubre, Madrid, 1977, pág. 1-6.

(101) El ADerecho de autodeterminación informática@, tiene su origen en la famosa Sentencia del Tribunal Cons- titucional Federal Alemán, de 15 de diciembre de 1983, que resolvió el recurso presentado contra una Ley de 25 de marzo de 1982, sobre el censo demográfico, que se declaró insconstitucional en razón del número de informaciones que solicitaba de sus ciudadanos. El Tribunal, --como lo comenta ORTI VALLEJO--, extrajo del derecho fundamental al libre desarrollo de la personalidad, la competencia de disponer sobre la revelación y el uso de sus datos personales. Como dice Podlech la autodeterminación informática junto con la libertad general de acción derivan del derecho al libre desarrollo de la personalidad. En cuanto al contenido del derecho de autodeterminación informática, Denninger aclara que la revelación y el uso de los datos personales, abarca todas las fases de elaboración y uso de datos, o sea, acumulación, transmisión, modificación y cancelación@. Vid. ORTI VALLEJO, A. EL DERECHO A LA INTIMIDAD E INFORMATICA... Ob. cit., pág. 39-40.

nuevo (a la Alibertad informática@,Aintimidad informática@,Aautodeterminación informática@), ni menos que este sea fundamental y autónomo de la misma intimidad, sino una visión, faceta o bastión tecnológico de la intimidad o de cualquier otro derecho fundamental.

En efecto, la visión iusinformática, como tal, es viable y aplicable al derecho a la intimidad como al conjunto de derechos fundamentales que lo soporten, pues constituye una faceta especial más para cada derecho al cual se analice, aplique y adicione. Así, podremos estudiar la visión iusinformática del derecho al honor, a la honra (art.21 Cons.Col.), la propia imagen, al buen nombre (art.15 Cons.Col.), etc. Esta investigación analiza la visión iusinformática de la intimidad.

3. ESTRUCTURACION DE LA VISION IUSINFORMATICA DEL DERECHO A LA INTIMIDAD.

Para configurar la visión iusinformática de los derechos fundamentales, aplicable también al derecho a la intimidad, debe tener en cuenta los siguientes elementos estructurales: El contenido del derecho de cada derecho (en este caso, de la intimidad); El concepto de *habeas mentem* (Derecho a la libertad genérico de toda persona, y en particular al derecho de la libertad de información); El derecho de origen anglosajón denominado de control de la información por sí mismo; Las facultades inherentes al habeas data (acceso, actualización, rectificación, bloqueo y cancelación de datos); y, finalmente los derechos de información previa al tratamiento informatizado de los datos considerados personales y el derecho de oposición al tratamiento y procesamiento informático, electrónico o telemático. Estos dos últimos derechos de originarios de las normas comunitarias europeas (Convenio 108 de 1981 y Directiva 95/46/CE) y españolas especiales (LORTAD., L.O.5/1992, arts. 5 y 13), dirigidos exclusivamente a la etapa preinformática (que es manual por esencia, pero que puede ser informatizada por excepción v.gr. Datos personales históricos, estadísticos, y archivísticos) e informática (en el curso del tratamiento o procedimiento informático se puede ejercitar el derecho de la información o el de oposición al tratamiento, tal como precisaremos más adelante).

3.1. *La Intimidad, el habeas mentem y el habeas data: Alibertad informática@.*

Retomamos el concepto de libertad informática, como base inicial de la visión iusinformática del derecho a la intimidad, sin considerarla un derecho fundamental autónomo. En efeto, el profesor Morales destaca tres esferas detectables del contenido de la intimidad: *a) La esfera íntima*. Incluyen las facultades clásicas de exclusión de terceros en lo que respecta a hechos o circunstancias relativas a la intimidad, con relevancia jurídica (secretos documentales, secretos domésticos, inviolabilidad de domicilio, etc) y otros derechos reconocidos en la Constitución, como el derecho de la contracepción, a la libertad sexual y el aborto en determinados casos. Estas facultades conducen a la evitación de cualquier tentativa de abstraer el

derecho de la intimidad del contexto en el que la privacy se imbrica con el *habeas mentem* o libertad genérica de la persona.

b) *La privacy frente a las libertades políticas.* En la sociedad tecnológica el carácter de garantísta de la privacy frente a otras libertades políticas previstas en la Constitución y el ordenamiento jurídico, la salvaguarda de la esfera íntima puede evitar el menoscabo de las dichas libertades. El carácter de garantista frente al control que facilitan los medios de vigilancia electrónica, por ejemplo. La privacy manifiesta un contenido positivo que se inserta implícitamente en cada una de las libertades y derechos fundamentales, tales como el derecho de asociación, libertad religiosa o de conciencia, derecho de sindicación, etc. , respecto de las que constituye un presupuesto lógico.

c) *Privacy frente a las libertades individuales.* La protección de los derechos y libertades fundamentales de la persona humana, por parte del Estado y por los mismos particulares, constituyen esta importante esfera de la intimidad. Inicialmente se hace aquí más evidente, el *habeas mentem*, pues late en el ambiente aquél derecho a la libertad sin injerencia alguna venga de donde proviniera.

El profesor Morales, a título enunciativo, propone como parte integrante de la esfera de la intimidad la protección de garantías constitucionales relativas al cuerpo humano, al domicilio, el derecho de defensa (confidencialidad y sigilo de la relación entre abogados y cliente), la presunción de inocencia y el derecho de silencio. De principio inmunes a toda clase de injerencia no prevista en el ordenamiento jurídico.

En las tres esferas Ael contenido positivo de la intimidad se determina el entronque del mismo con la libertad personal. No obstante, con ello no se completa el cuadro lógico de facultades que dimanan de la privacy. Construcción unitaria de esta esfera de protección debe superar la fase preinformática para completar el estatuto jurídico del *habeas data*@ [102]. En la fase informática el *habeas mentem* esta estrechamente ligado con el desarrollo que las tecnologías informáticas han conseguido en esta sociedad informatizada o A*cibernética*@[103]: Aen esta fase de la

evolución del derecho a la intimidad, la libertad informática constituye el fundamento del habeas data@. Lo anterior, prueba una vez más, no sólo la ambigüedad en el contenido del derecho a la intimidad sino en su amplia Aversatilidad@ y adecuación a los momentos históricos y cambios tecnológicos que se producen en la sociedad.

En este momento de la conceptualización del derecho a la intimidad se identifica a éste con la llamada *Alibertad informática@*, por el advenimiento de las nuevas tecnologías de la información y la comunicación (TIC), pero sobre todo, por el ejercicio pleno de las libertades fundamentales del individuo, de principio para poder acceder a todo tipo de información (almacenada y tratada manual o informáticamente) sea cual fuere la persona que la tenga (natural, jurídica, pública o privada), siempre que sea sobre sí mismo o que le concierne, a efectos inmediatos de consultar o revisarla, y fruto de aquéllas facultades, solicitar, sí fuere del caso, la rectificación o la cancelación de la información, si resulta inexacta o incorrecta (fundamentación teórica del habeas data).

Desde este punto de vista, la facetas preinformática e informática del derecho a la intimidad, se basan exclusivamente en el *habeas mentem* y el *habeas data*, los cuales conforman el derecho a la *Alibertad informática@*, vale decir, el derecho de toda persona para ejercitar el derecho habeas data (acceso, rectificación y cancelación de los datos), cuando la información le concierna y esta es inexacta o ilegal.

---

(102) MORALES PRATS, F. Ob.ut supra cit., pág. 125.

(103) El término de cibernética cumplió su cometido dentro de la fase de evolución de la informática general y de la informática jurídica en particular en la década de los 60´s y 70´s , tal como precisaremos en la Parte III de este ensayo socio-jurídico. La cibernética destaca una de las facultades básicas de los ordenadores o computadores, cual es el almacenamiento y la capacidad de organización de todo tipo de información. En esta época se conocen los trabajos de los italianos MARIO LOSSANO: A*Guiscibernética, in Nouvi sviluppi della sociologia del diritto 1966-1967*" y de VITTORIO FROSSNI: ACibernética, diritto e societá@ (1968). En España, la cibernética unida a al derecho, conformó la Aiuscibernética@ que tanto comenta el iusinformático español Manuel LOPEZ MUÑIZ-GOÑI, en su obra: *Informática jurídica documental*, 1983. Años después se ampliarían dichas funciones conservativas de información a otras Alogiciales@ como las de Aencadenamiento lógico de la información@, Ala intercomunicación entre computadores@ de imágenes, sonidos o texto: su principal aplicación la multimedia, la Ainformática decisional@, etc.

El Tribunal Constitucional de España, en Sentencia No.254, de 20 de Julio de 1993, resume esta postura:

> *APues, como señala el MF, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada *libertad informática+, es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)@* (F.J. 7) [104].

3.2. El derecho al control de la información referente a uno mismo (*The Right to control information about oneself*): En las leyes de protección a laAPrivacy@ y la protección al derecho de la libertad de información.

3.2.1. En el Common Law norteamericano.

Pese a argumentación generalizada *contrario sensu*, este derecho de control de la información de sí mismo, expresamente se halla previsto en el ensayo socio-jurídico de Warren y Brandeis, tal como lo denotábamos al hacer referencia al aspecto negativo (facultades de exclusión: The right to let alone), como el aspecto positivo de autocontrol de la información, basado en que el *Common law* garantizaba por desde aquélla época el derecho Aa toda persona a decidir hasta que punto pueden ser comunicados a otros pensamientos, sentimientos y emociones@ --Asi expresan por escrito, o mediante una actuación, una conversación, por aptitudes o por un gesto@-- (igualmente tiene derecho a reservárselos, Aa juzgar si quiere hacerlos públicos o manifestarlos únicamente ante sus amigos@Miller vs.Teylor), al igual que en Ala tranquilidad de espíritu y en el alivio que proporciona el poder impedir la publicación@ de una obra del intelecto humano, un libro, obra de arte, etc, por parte de su autor, y en concreto al A derecho de una persona particular a impedir que su retrato circule, el derecho a estar protegido de los retratos hechos a mano, el derecho a estar protegido de un debate sobre un asunto privado@ y que Alas relaciones sociales y familiares (estén sometidas) ante una publicidad despiadada (*My home is my castle)@.* Estas facultades inherentes al derecho a la Aprivacy@, en

Warren y Brandeis, no son sino una extensión a nuevos hechos (como los comentados

---

(104) Sent 254/1993. M.P. García Món. TC, Sala 1. Vid. AA.VV. COMPENDIO DE DISCOS ARANZADI... Ob. cit. 1998.

en el ensayo), y que hacen A parte de un derecho más general el de A*la inviolabilidad de la persona* --del derecho a la propia personalidad--@ [105].

Estas facultades de la Aprivacy@ no son absolutas, sino limitadas por el propio *common law*, según Warren y Brandeis, en Ala exacta frontera en que la dignidad y la conveniencia del individuo deben ceder ante las exigencias del bienestar general o de la equidad@ y estas a título enunciativo son:

> ***1***. *El derecho a la intimidad no impide la publicación de aquello que es de interés público o general.* ***2***. *El derecho a la intimidad no prohíbe la información sobre un tema, aun siendo éste de naturaleza privada, si la publicación se hace en las circunstancias en que, conforme a la ley de difamación y libelo, sería calificada de información privilegiada.****3***. *El derecho no otorgaría, probablemente, ninguna reparación por violación de la intimidad cuando la publicación se haga en forma oral y sin causar daños especiales.****4***. *El derecho a la intimidad decae con la publicación de los hechos por el individuo, o con su consentimiento. Esto es una aplicación de la ley de propiedad literaria y artística.* ***5*** *La veracidad de lo que se publica no supone una defensa. Se impide es la publicación incorrecta de la vida privada y el que pueda ser descrita. 6 La ausencia de ´malicia´en quien hace público algo no constituye defensa*[106].

En forma sintética los planteamientos de Warren y Brandeis, se recogen por La *Office of Science and Technology of the Executive Office of the President@* de los EE.UU, 1967, cuando emite un concepto sobre la Aprivacy@ en los siguientes términos: Ael derecho a la vida privada es el derecho del individuo de decidir por sí mismo en que medida compartirá con otros sus pensamientos, sus sentimientos y los hechos de su vida privada...@ [107]

Posteriormente la doctrina conoce los trabajo de *Westin* en 1967 (*Privacy and Freedom*) y *Shattuck*, en 1977 (*Rights of Privacy*), sobre el derecho al control de la información referente a uno mismo, autores que han tenido el mérito de poner de relieve una progresiva tendencia a concebir la Aprivacy@ como el poder de ejercer un control sobre las informaciones que puedan afectar al individuo [108].

---

(105) WARREN, Samuel y BRANDEIS, Luis.. *EL DERECHO A LA INTIMIDAD.* Ed.Civitas, S.A., Trad. Benigno Pendás y Pilar Baselga, Madrid, 1995. págs. 45 y ss.
(106) Ibídem, pág. 61 a 69.
(107) LOPEZ DIAZ, E. Ob.cit., pág.189.
(108) Ibídem, pág. 189

Los estudios de *Westin* y *Shattuck* se fundan en el impacto de las nuevas tecnologías de la información (TI), el avance de los sistemas informáticos basados en los computadores u ordenadores, en las libertades fundamentales e intimidad y en el derecho de acceso a la información, tal como puntualizamos en las notas de pie de página 44 y 76. Desde aquella época se pone en evidencia la irrupción de las tecnologías, la informática no sólo en la potencial vulnerabilidad de los derechos y libertades que con ella se posibilitan sino en la igualmente potenciada protección que con aquellas puede logarse si se actúa conforme al *Common Law*. Con el paso del tiempo, son más los argumentos a favor del riesgo, la ampliación del grado de vulnerabilidad y Ala amenaza@ que representan estas nuevas tecnologías y la informática que los argumentos proteccionistas, y así quedará plasmado en las diferentes legislaciones y Constitucionales del mundo.

La matización de *Shattuck* al derecho de control de la información sobre sí mismo, queda representada en su trabajo, cuando expone que no sólo las personas individualmente representadas tienen y pueden ejercitar dicho derecho, sino también las personas consideradas como A grupos@ [109]. Entendemos que se refería a las personas jurídicas colectivas (privadas o públicas), lo cual plantea la posibilidad del derecho al control de la información (A*information control*@) de las personas

jurídicas y no sólo las personas físicas o naturales, como había sido la tesis dominante hasta ese momento de la evolución del aquél derecho y de los derechos fundamentales en general (v.gr. La Jurisprudencia de la Corte Constitucional colombiana, se reconoció a partir de 1993 [110]) .

---

(109) Ibídem, pág. 206

(110) Una de las formas idóneas, en el actual derecho de controlar la información de uno mismo, es a través del ejercicio del derecho de habeas data. Por ello, conviene transcribir la Sentencia T-462, de 24 de Septiembre de 1997 del TRIBUNAL CONSTITUCIONAL COLOMBIANO, que reitera jursiprudencia anterior sobre la materia. A2. *El Derecho al Habeas Data de las Personas Jurídicas*. En relación con la condición de titulares de derechos fundamentales que ostentan las personas jurídicas, esta Corporación, en reiterada jurisprudencia, que una vez más se repite, ha afirmado que por ser capaces de una voluntad racional y autónoma, estos entes colectivos son verdaderas personas en sentido jurídico, esto es titulares de derechos y obligaciones y, en especial, titulares también de derechos fundamentales. En este sentido, en la sentencia T-396 del 16 de septiembre de 1993 se expresaron los siguientes conceptos:*"La persona jurídica es apta para la titularidad de derechos y deberes por su racionalidad y por su autonomía. La aptitud es la adecuada disposición para dar o recibir, para hacer o soportar algo, y la persona jurídica puede (tiene la dimensión jurídica de la facultad) y también debe (soporta el deber frente a sus miembros y frente a otras personas jurídicas o naturales); por tanto tiene adecuada disposición para que se le otorguen o reconozcan derechos y deberes. "La racionalidad y la autonomía hacen que la persona jurídica sea apta para el mundo de los derechos, de los deberes y de las relaciones jurídicas según un principio de igualdad, aunque no de*

En términos de *Westin,*)qué facultades comprendía ese derecho a controlar la información uno mismo?

De la radiografía de hechos, sucesos, derechos y avances tecnológicos de la sociedad Norteamérica de aquella época descritas en su libro A*Seguridades legales para*

--- Continuación de la nota 110 --

identidad absoluta. "Este tipo de entidad al ser racional y autónoma es por sí (per se), no por otro, es decir, es persona (personare). De alguna manera es substancial; y todo lo substancial es un supuesto, y el supuesto es sujeto, y si éste es racional y autónomo, sin duda alguna tiene que ser sujeto de derechos y deberes. Luego la persona jurídica es una entidad que se expresa jurídicamente como sujeto de derechos y deberes". (...) "Los derechos fundamentales son aquellos que fundan la legitimidad del orden jurídico, por tratarse del reconocimiento que el sistema legal positivo hace unos bienes que son necesarios para la dignidad de la vida humana puesta en relación social. Estos derechos son necesarios, no contingentes tanto para el orden social justo, como para el despliegue jurídico adecuado de la persona. Tuvo el sistema ius filosófico que acudir al origen remoto de tales derechos en el ius naturale que era exclusivo para la persona humana. Luego vino un concepto más depurado, que se fundaba no tanto en la naturaleza humana, sino que se centraba en la dignidad de la persona y surgió el criterio de los derechos individuales del hombre, que luego admitió la socialidad y solidaridad de éste, de suerte que desembocó en los derechos colectivos de las personas, y aquí se encuadra, por vez primera, la titularidad de las personas jurídicas como sujeto de derechos fundamentales, como expresión mancomunada de la idea social de los seres humanos, que tienden a vincularse por medio del derecho, en lugar de disociarse en aras de una mal entendida individualidad. Con el advenimiento de la segunda generación de derechos humanos -que incluye lo social como sujeto de derecho- se consolida hoy, en la vigencia plena de la llamada tercera generación de derechos humanos (derechos de los pueblos y reconocimiento de la humanidad como gran persona jurídica sujeto de derecho universales), es contra evidente afirmar que sólo los individuos considerados aisladamente son titulares de los derechos fundamentales, porque ello supone negar toda una evolución jurídica trascendente, en el sentido de que el hombre se realiza como persona también en forma colectiva, y para ello necesita de la protección jurídica tanto desde su dimensión universal, como de su aspecto

en sociedades autónomas. (M.P.: Dr. Vladimiro Naranjo Mesa)," Estando pues claramente establecido que las personas jurídicas son titulares de derechos fundamentales, y por lo tanto de la acción de tutela, resulta necesario precisar, adicionalmente, que de manera específica son titulares del derecho de habeas data; en ese sentido, en la misma Sentencia, se dijo lo siguiente:"La persona jurídica no es titular de los derechos inherentes a la persona humana, es cierto, pero sí de derechos fundamentales asimilados, por razonabilidad, a ella. No tiene el derecho a la vida, pero sí al respeto a su existencia jurídica (Cfr. art. 14 C.P.). Igualmente, se encuentra que por derivación lógica, por lo menos, es titular de derechos constitucionales fundamentales, los cuales se presentan en ella no de idéntica forma a como se presentan en la persona natural. A título de ejemplo, en una enumeración no taxativa, se tienen los siguientes "- El derecho a la libertad, en el sentido de poder obrar sin coacción injustificada con conciencia colectiva de las finalidades. "- El derecho a la propiedad, ya que es una característica esencial de la persona el ser dueña de sí, y, en dicha autoposesión tiene la capacidad de apropiación de cosas exteriores, en las cuales o por medio de las cuales manifiesta la expresión de su personalidad. Toda persona necesita de la propiedad para ejercer su capacidad esencial de apropiación. "- El derecho a la igualdad en derecho y a tener condiciones de proporcionalidad en las relaciones con otros sujetos de derecho. Sin la existencia del derecho a la igualdad, se hace imposible la relación de justicia, y como la persona jurídica debe existir en la realización de un orden social justo, se colige que necesita del derecho a la igualdad. "- El derecho al buen nombre, porque es un elemento de trascendencia social, propio de todo sujeto de derecho, que busca el reconocimiento y la aceptación social, con el fin de proyectar nos sólo su imagen, sino su mismo ser en la convivencia social. Las personas naturales que conforman la persona jurídica se verían afectadas si el todo que las vincula no es titular del buen nombre como derecho. Hay un interés social que legitima la acción de reconocimiento, por parte del Estado y de la sociedad civil, del buen nombre que ha adquirido un ente colectivo, porque ello necesariamente refleja el trabajo de las personas humanas en desarrollar la perfección de un ideal común objetivo." Si las personas jurídicas son titulares del derecho fundamental al buen nombre, en consecuencia lo son también del derecho al habeas data, toda vez que este último derecho, reconocido por el artículo 15 de la Carta Política, existe justamente como garantía de aquel y del derecho a la intimidad personal y familiar. En efecto, la sola lectura del texto constitucional mencionado, pone de relieve que el habeas data, entendido por el constituyente como el derecho de las personas a "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas", se vincula directamente con los derechos a la intimidad y buen nombre a los que se refiere el primer enunciado del artículo superior en comento. De esta manera, el habeas data viene a ser como una garantía de estos dos derechos, siendo por lo tanto accesorio de ellos@. Texto completo en: *WWW.RDH.GOV.CO* (Base de Datos de la Red Nacional de Derechos Humanos de Colombia). 1998.

garantizar la intimidad en una sociedad de computadores, 1967" **[111]**, se deducen los siguientes:

a) Partiendo de un supuesto cierto del concepto de Ainformación personal@ que Ano ha tenido ningún sistema general para tratar el flujo de información que controlan los órganos de gobierno,... excepto algunos... datos censales,... de cargas fiscales... tenemos tradición de libre circulación de información... tenemos tradiciones de carácter confidencial y reservas mantenidas en secreto..@

b) La ley norteamericana Ano ha desarrollado procedimientos institucionales para la protección contra la recogida inapropiada de información, almacenamiento de datos inadecuados o falsos, y empleo entre organizaciones de dicha información@.

c) El Acta de Procedimiento Federal de 1946, Aaseguraba a los hombres de negocio que se enfrenten con órganos reguladores federales@, lo siguiente: 1. Conocer Ala información que sobre ellos iba a entrar en los expedientes...@, 2. Que Atendrían otra oportunidad de presentar otra información para *recusar* (-sic-. puesto que la traducción más coherente con el contexto, sería rehusar) o modificar esa información@; y 3. Como consecuencia de lo anterior, Ael expediente... sería sometido a revisión@.

En síntesis, el derecho a controlar la información de sí mismo, cuando haya sido recogida o almacenada en forma de datos inadecuados o falsos por las autoridades gubernamentales , se extiende a las facultades de conocer, acceder, revisar, modificar o rehusar dicha información.

Con posterioridad, la *Privacy Act, 1974* (Ley de la privacidad, traducida por Fariñas [112]), sostiene que Afinalidad de la presente ley es establecer medidas de protección contra la invasión de la privacidad personal@, previamente considerando que:

> *La privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de la información personal por entes y órganos federales. El creciente uso de orde-*

---

(111) Se Castellaniza la APrivacy@ por privacidad. FARIÑAS MATONI, L., Ob. ut supra cit., pág. 151-152.
(112) Ibídem., pág. 156.

> *nadores, esencial para el funcionamiento de las Administraciones públicas, ha aumentado el detrimento de la privacidad individual. El derecho de la privacidad es un derecho personal y fundamental protegido por la Constitución.*

En la parte pertinente, al derecho a controlar la información sobre uno mismo y el ejercicio subsecuente de las facultades que éste engendra en entronque con el *habeas data*, la *Privacy Act*, sostiene: El órgano que llevare un sistema de registros (entendiendo como registro, una unidad de información personal tratada, almacenada y registrada informáticamente con el consentimiento expreso de la

persona concernida) deberá permitir al individuo examinar y tomar nota del registro a él concerniente y permitirle solicitar modificaciones.

En consecuencia, según la *Privacy Act*, todo órgano que llevare un sistema deberá:

> *1) conservar sólo aquella información relevante y necesaria; 2) recogerla a ser posible directamente del interesado; 3) informar a quien requiriese a facilitar información de: i) la autorización que permitiere solicitar la información, ii) de la finalidad, de los usos de trámite; y iii) de las consecencias de no facilitar información; 4) Publicar en el Registro Federal una nota acerca de la existencia y carácter del sistema de registro; 5) llevar los registros con exactitud; 6) garantizar la exactitud; 7) no llevar registro sobre cómo el individuo ejerciere derechos garantizados por la Primera Enmienda (religión, libertad de palabra y prensa, reunión pacífica, reparación de agravios); 8) dar cuenta al individuo cuando el registro fuere puesto a disposición de una persona en razón de mandamiento judicial; 9) formular normas deontológicas para las personas ocupadas en los registros; 10) garantizar la seguridad y confiabilidad; y 11) publicar en el Registro Federal el aviso de cualquier nuevo uso de la información contenida* [113].

3.2.2. En la AFreedom of information Act@--FOIC-- de Australia.

En Australia, se regula el derecho de control a la información de sí mismo y las facultades subsecuentes de actualización, rectificación y cancelación de la información

---

(113) Se establece como regla general en la *Privacy Act, 1974,* que Aningún órgano revelará registro (o información personal codificada) alguno a nadie, excepto con petición escrita o consentimiento escrito del individuo al que perteneciere el registro, salvado que la revelación fuere hecha: 1) a directivos y empleados del órgano que llevase el registro para cumplimiento de sus deberes; 2) para usos de trámite; 3) a la Oficina del Censo; 5) a quien hubiere facilitado compromiso escrito de que el registro será usado solamente como dato de investigación o información estadística; 6) a los Archivos Nacionales de los Estados Unidos; 7) a otro órgano parqa aplicación de leyes civiles o penales si estuviere autorizado y hubiere formulado petición escrita; 8) a una persona si se probare la existencia de circunstancias poderosas que afectaren a la salud o seguridad de un individuo; 9) a una de las Cámaras del Congreso; 10) al Interventor General o sus delegados en funciones de la oficina General de contabilidad; 11) por madamiento del Tribunal competente@. Vid. FARIÑAS MATONI, L., Ob. cit., pág. 156.

Ainexacta, incorrecta, desactualizada o no puesta al día (*out of date*) o falsa (*misleading*)@, en el art., 51A, de la AFreedom of information Act 1982" [114]. Esta ley regula en forma amplia el derecho a la libertad de información, y por supuesto,

incluye el derecho de acceso a los documentos públicos (Parte III, arte. 11 a 31), las excepciones al mismo (Parte IV, arte. 32 a v.gr. por seguridad, defensa o relaciones internacionales), el acceso a la información de carácter personal (Parte V, art.48 a 51E), y la revisión y procedimientos en vía administrativa y jurisdiccional por el quebrantamiento de este derecho (Parte VI, art. 52 a 66).

3.2.3. En la AAcces to information Act --ATIA-- del Canadá.

En la *Access to information Act, --ATIA--* 1980-1983 del Canadá [115], regula lo atinente al derecho de la información, extendiendo los derechos de las personas sobre el acceso a la información o datos personales y generales (sin limitar ni restringir la información disponible y de acceso público) que se hallen bajo el control de las autoridades gubernamentales. El principio básico de la ATIA, es la codificación del derecho de acceso público a la información, garantizada a todo ciudadano nacional o extranjero residente, siempre que esté bajo el control del Gobierno canadiense. El derecho de acceso no tendrá ninguna interdicción, limitación o restricción, excepto cuando los tribunales y la ATIA en casos expresamente previsto así lo prevea. Por eso el derecho de acceso no es absoluto (Rubin v. Canadá, 1994,Tribunal Federal).

En amplio glosario de definiciones con el que inicia la ATIA, se define lo que se entiende por Ainformación personal@ (art. 3 y 19), Arecord@ o Aregister@ (como unidades de información procesada informáticamente), así como establece los casos de descubrimiento y divulgación de la información previos unos requisitos generales y especiales (arts. 8-2 y 19-2). Todo ello comentaremos a espacio en la parte III de esta investigación.

---

(114) Vid. Texto completo en WWW.AUSTLI.EDUC.CO
(115) Vid. Texto completo en: WWW.UMONTREAL.EDU.CA.

Por ahora, respecto del *Right of access* la ATIA, regula a partir del art.4, 4-3, (reformados parcialmente en 1985 y 1992) a art. 12 el derecho de acceso a la información personal codificada informáticamente y contenida en bases de datos (o Arecord@), estableciendo unos requisitos de forma (v.gr. Petición de la persona interesada o titular de la información, idioma o en formato alternativo, si se trata de Adeficientes sensoriales@), de contenido (v.gr. La información debe estar bajo el control gubernamental) y temporales. Así, según la clase de información, contenido e interés se establecen períodos de tiempo para ejercitar el derecho de acceso, al igual que para denegarlo, o para no acceder a descubrirla o divulgarla (Adisclosed@) si se realiza por fuera de estos parámetros legales (art.10). La información personal confidencial obtenida de por el Gobierno tendrá diferente tratamiento, pues sólo puede descubrirse cuando haya consentimiento expreso del titular (art.13), o cuando expresamente esta previsto en la ATIA (art.19) dentro de las cuales se incluye las ordenes de los Tribunales Judiciales. El Comisionado para la protección de la información (*The information Commissioner*), protegerá la vulneración de los preceptos de la ley y tiene facultades investigativas, correctivas y sancionatorias en vía administrativa.

3.2.4. En el AEstatuto del derecho a la Información@ y la Constitución Colombiana de 1991.

En el Derecho Colombiano, las normas que regulan el derecho de acceso a la información general y personal, con carácter preconstitucional a la Constitución de 1991 y contenida en documentos u otros instrumentos que se asimilen (los discos electromagnéticos, planos, fotografías, etc. art.252 Código de Procedimiento Civil), se encuentra regulada en la Ley 57 de 1985 (que amplia el derecho ya plasmado en la Ley 4 de 1913, art.342) para los documentos públicos. La ley 16 de 1972, de 20 de diciembre (que regula el derecho a la información y en forma especial el derecho a rectificación y respuesta) y el Código Contencioso Administrativo (C.C.A de 1984-89) para el acceso a los documentos por origen o asimilación (incluidos los documentos informáticos, electrónicos y telemáticos) o cualquiera otro que contenga

información pública o de carácter particular. El derecho control a la información de uno mismo, siguiendo el ejemplo de las leyes norteamericanas, las normas internacionales (Pacto de San José y de New York, principalmente) y la ATIA canadiense, se concreta a los derecho de conocimiento de la información y el ejercicio de los derechos subsecuentes de actualización, rectificación y modificación, si las informaciones son Ainexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirigen al público en general@ (art. 14 Ley 16/72). Conjunto de normas conocidas como el AEstatuto del derecho a la Información@ [116].

Sólo con el advenimiento de la Constitución de 1991, se vino a plasmar en forma expresa y ampliada, *el derecho a controlar la información sobre sí*, tras elevar a rango constitucional el derecho de *habeas data*, y por tanto, toda información que le concierna a una persona y esté bajo el control de los poderes públicos o de particulares, podrá ser actualizada, rectificada o cancelada, sea cual fuere el formato en el que estén recogida, almacenada, transmitida o difundida, es decir, por mecanismos manuales o informáticos (art. 15 , 73 y 74). Así se completó el cuadro preconstitucional y constitucional del control a la información de sí mismo en el derecho colombiano.

El derecho fundamental a la información previsto en los arts. 20, 73, 74 de la Cons.Pol. (CC., Sent. T-080, Feb.26/1993 y Sent. SU-082/1995), y el derecho igualmente fundamental de *habeas data* (art.15 y 74), reglamentados preconstitucionalmente por el conjunto de normas anteriores, han sido suficiente instrumento de tutela y protección idóneos en el derecho colombiano para preservar y garantizar la visión iusinformática del derecho a la intimidad, como la de otros derechos, tales como: el del honor, la honra, el buen nombre e incluso el libre desarrollo de la personalidad. Aunque es oportuno reconocer que el legislador colombiano desde 1991, ha intentado regular el procedimiento informatizado de datos personales de carácter económico, financiero y bancario privado, a través de diversos proyectos de ley que no han hecho curso en el Parlamento, por diversas

razones jurídicas, y especialmente, porque se pretende regular este procedimiento sólo con base en las facultades inherentes

---

(116) El art. 20 de la Cons.Pol., de 1991., prescribe: ASe garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, *la de informar y recibir información veraz e imparcial,... Se garantiza el derecho a la rectificación en condiciones de equidad@.* Sobre El derecho a la información en el orden constitucional y reglamentario, en forma amplia, en mi trabajo: *LA CONSTITUCION DE 1991*... Ob. cit., págs. 7 y ss.

al derecho de habeas data (acceso, rectificación y cancelación de datos), sin contextuarlo con el derecho a la información, los valores constitucionales de la dignidad humana y el interés general (art. 1 Cons.Pol), los límites a todo derecho fundamental (Arespeto a los derechos ajenos y no abusar de los propios@ y Adefensa de los derechos humanos como fundamento de la convivencia pacífica@ art. 95-1 y 4., Cons.Pol), el contenido esencial del derecho fundamental (v.gr. La interdicción a declarar contra sí mismo Acónyuge, compañera@o sus parientes, art.33 Cons.Pol) y el principio constitucional de reserva legal (regulación de derechos fundamentales y procedimientos de éstos, sólo por Ley Estatutaria art.152-a Cons. Nal). Todo ello, por cuanto el objeto principal de la Ley Estatutaria (norma integral sobre la materia) es reglamentar derechos fundamentales (la intimidad, el buen nombre, el habeas y el de información) que se ven involucrados con el acceso, utilización y transferencia de datos personales por medios informáticos, electrónicos y telemáticos en lo que hemos denominado visión iusinformática de los derechos y libertades fundamentales.

El último proyecto de Ley 127/1993, que cursó en el Parlamento y Apor el cual se dictan algunas disposiciones sobre el ejercicio, de la actividad de recolección, manejo, conservación y divulgación de información comercial@, fue declarado inconstitucional por parte de la Corte Constitucional, por vicios de forma al no haberse conformado el quórum decisorio en el Congreso para votar proyectos de ley estatutaria, que regulan derechos fundamentales como el Aderecho de habeas data@[117]. En cuanto al contenido, el proyecto sostenía protuberantes fallas, tales como: Enmascarar la regulación del

---

(117) La Corte Constitucional Colombiana, con base en el control previo de constitucionalidad sobre los proyectos de leyes estatutarias (arts. 153 y 241.8), declaró inconstitucional el proyecto de Ley 127/1993. Dicho proyecto contenía, lo siguiente: Protección de la Intimidad y el buen nombre (art.1), Ambito de aplicación (art.2), Legitimidad de las bases de datos (art.3), Reglas de funcionamiento (art. 4), Calidad de la información (art. 5), Responsabilidad (art. 6), Fuentes legitimas de información (art. 7), Exactitud de la información (art. 8), Eliminación de registros (art.9), Suministros de información (art.10), Información de circulación restringida (art. 11), Caducidad de los registros (art.12), Responsabilidad de las fuentes de información (art.13), Acciones de tutela (art.14), Suministro de información fuera del país (art.15), Excepciones (art.16), Determinación de la responsabilidad (art.17), Vigencia (art.18) Este proyecto de ley retoma algunos conceptos e instituciones jurídicas previstas en el Reglamento de la Asociación Bancaria y de entidades financieras de Colombia --ASOBANCARIA--, aprobado por su Junta Directiva, el 23 de Marzo de 1995 y que rige actualmente para el sector bancario y financiero y cuenta con una Central de Información --CIFIN--, como un servicio privado, de interés público, de información del sistema financiero colombiano. Esta formado por las bases de datos de carácter personal económico que la Junta Directiva estime necesario para servir a las instituciones usuarias como un elemento de juicio por considerar en la evaluación de riesgo de los negocios financieros y operaciones activas de crédito que celebren con sus clientes (art. 1 y 2). Texto del proyecto citado en la Sentencia de la Corte Constitucionsal T-095/1995, de 17 de Enero. En: *WWW. RDH.GOV.CO*. 1998.

tratamiento informatizado de datos personales generales, en la regulación específica de los datos personales de carácter económico, con lo cual, además de extralimitar los parámetros constitucionales y legales sobre la materia, se incurría en una evidente falta de unidad temática del contenido y violación de la reserva legal sobre la materia regulada. Con base en dicho solapamiento temático del proyecto, salen en cascada los defectos que violan el contenido esencial del habeas data y derecho a la intimidad, pues se regulaba, sobre aquello que la doctrina, jurisprudencia y legislación universal ha proscrito de reglamentarlo como son los datos del núcleo esencial de la Aprivacy@; y en el evento exceptivo de hacerlo, con precisas y excepciones *numerus clausus*; en fin, otros aspectos que a lo largo de la investigación iremos apuntando.

3.2.5. En el Derecho Europeo en las Leyes de Protección de Datos.

En el derecho Europeo, principalmente en Alemania y Suecia, en la década de los 70´s, conservan directrices conceptuales sobre *el derecho a controlar la información de uno mismo*, así como de las facultades subsecuentes a través de las leyes que protegen Alos datos@ en general y en concreto, los de carácter particular, de aquellos datos que han sido tratados (recogidos, almacenados, conservados o difundidos) mediante soportes, medios o aplicaciones informáticos. Así, la Ley Federal Alemana de Protección de los Datos Personales de 1977, de 27 de Enero, modificada parcialmente en 1990, tal como puntualizaremos más adelante. En efecto, esta Ley, reconoce una serie de facultades a toda persona a quien le

concierne una información personal tratada informáticamente, tales como el de conocer los datos almacenados en una base de datos, de rectificarlos si fueren inexactos, de bloqueo cuando no fueren exactos o cuando no se hubieren dada las condiciones originales para las cuales se requiere su almacenamiento y de cancelación, si el almacenamiento no hubiere sido admisible o bien --a elección , además del derecho de cancelación-- cuando dejaren de darse las condiciones que originalmente requieran su almacenamiento (art.4) [118] .

En la Ley Orgánica de regulación del tratamiento automatizado de los datos de

---

(118) Texto completo en: RIVERA LLANO, Abelardo. *DIMENSIONES DE LA INFORMATICA EN EL DE- RECHO (PERSPECTIVAS Y PROBLEMAS).* Ed. Jurídica Radar, Santafé de Bogotá, 1a., ed., 1995.

carácter personal (LORTAD: L.O.5/1992, de 29 de Oct), como se puntualizará más adelante, este derecho a controlar la información de uno mismo, toma especial connotación pues se establece con condición *sine qua nom* para el ejercicio del conjunto de facultades que desencadena este derecho (actualización, rectificación, bloqueo y cancelación de los datos personales), una principio-derecho que denominamos Ade información previa@ (art.5 y 13), en Amodo expreso, preciso e inequívoco@ (art.5-1) para todo tratamiento informatizado de datos, pero prioritariamente para la recogida de datos. Con base en este Aderecho de información@, la persona concernida tiene, entre otras facultades, la de conocimiento sobre la existencia Ade un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de *ejercitar los derechos de acceso* (arts. 14, para denegarlo arts. 15.5., 20 y 21 LORTAD., reglamentados por los arts. 12 y 13 del R.D.1332/94), *rectificación y cancelación* (art. 15 y 16 LORTAD., reglamentado por el art. 15 del R.D.1332 /94 [119]) y de conocer la identidad y dirección del responsable del fichero@ (o banco de datos informatizado).

3.3. El derecho de Habeas Data: como una cautela de protección de los derechos de los derechos fundamentales [120].

Como pudimos comprobar anteriormente una vertiente importante de los orígenes teóricos del habeas data se encuentran en aquél derecho del *Common Law* norteameri-

---

(119) El derecho de acceso consiste Aen la facultad o capacidad que se reconoce al afectado de recabar información de sus datos de carácter personal incluidos y tratados en los ficheros automatizados, en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo. El acceso podrá consistir en la mera consulta de los ficheros por medio de la visualización, o en la comunicación de los datos pertinentes por escrito, copia o telecopia, certificada o no. La información deberá ser legible e inteligible cualquiera que sea el medio utilizado.)Cómo se ejerce ese derecho?. Se ejercerá mediante solicitud o petición dirigida al responsable del fichero, formulada mediante cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar@. AA.VV. *MANUAL DE LA AGENCIA DE PROTECCION DE DATOS.* Textos de la normativa sobre datos personales (LORTA Y R.D. 1332/94) en AA.VV. *COMPEDIO DE DISCOS ARANZADI*. Ed. Aranzadi, 1997.

(120) El profesor MORALES PRATS, considera que los Aderechos que integran el *habeas data* y dotan a la tutela jurídica de la privacy de una impronta procesal-cautelar, también determinan una alteración de las facultades de exclusión preinformática del derecho a la intimidad@. Sin embargo, creemos que el carácter cautelar del habeas data esta instituido para el conjunto de derechos y libertades fundamentales, aunque con mayor incidencia para la protección de la intimidad. Quizá por ello, este énfasis proteccionista del habeas data a la intimidad ha marcado toda una época doctrinal, legislativo y Constitucional como veremos. Vid. MORALES PRATS, *LA TUTELA*...pág. 125.

cano denominado *AThe Right to control information about oneself@* por Alain Westin en 1967. Sin querer abrir debate sobre ello y más bien ubicar nuestra investigación en un esquema didáctico y consecuencial con nuestros propósitos, no abordamos otras vertientes del nacimiento del derecho de habeas data, para mejor aún, analizar los efectos que ha producido en la visión de iusinformática de los derechos fundamentales, y por su puesto en el derecho de la intimidad, desde su conceptualización doctrinal y jurisprudencial hasta su constitucionalización en varias Cartas Magnas del Derecho Occidental v.gr. En Portugal en 1976, en España en 1978, en Brasil 1988 [121], y en Colombia en 1991.

El derecho de habeas data, en un momento de su evolución conceptual fue considerado como el derecho de acceso a la información o los datos (cuando esta información fue codificada o tratada informáticamente) de carácter personal, a efectos de conocer; en primer término, la existencia de un fichero o banco de datos

(manual o informático), la existencia de datos referentes al accedente o peticionario (el concernido), la identidad de la persona (natural, jurídica, pública o privada) que tenía dicha información; y en segundo lugar, ejercitar las facultades consecuentes a ese conocimiento específico y finalístico, es decir, para que la información encontrada en estas condiciones, sea consultada, revisada o, en su caso, solicitar una copia de los documentos o elementos que se asimilan a éste (v.gr. discos, Acassettes@, fotografías, etc), para propósitos concretos posteriores. Quizá por ello, comenta el profesor *González Navarro* [122], que en un principio el derecho de acceso a la información fue bautizado de *habeas data*, por considerarlo una modalidad de acción exhitoria análoga a la del *habeas corpus.*

En el comentario doctrinal, legislativo y constitucional realizado en el aparte anterior, pudimos ver como el derecho al control de la información sobre sí mismo, desde la Privacy Act 1974 norteamericana hasta la actualidad, se fueron incorporando unas facultades consecuenciales inherentes a ese derecho que permitían su pleno y cumplido

---

(121) Vid. GONZALEZ NAVARRO, F. *COMENTARIOS A LA LEY DE REGIMEN* ... Ob. ut supra cit., pág. 711.

(122) Ibídem, pág. 711

ejercicio y desarrollo. Sintéticamente son: Conocimiento de la existencia de la información, quiénes la administran y controlan, los fines y objetivos para los cuáles fue recogida, almacena y tratada (en forma manual o informática), cómo, en qué momento, y para qué se consulta, revisa la información; y consecuentemente, si la información resulta, inexacta, incorrecta, indebida, falsa o ilegal, poder pedir la actualización, rectificación, bloqueo y cancelación, según fuere el caso y circunstancias particulares.

La Constitución Portuguesa de Abril 2 de 1976, expresamente instituyó el derecho de *habeas data*, en el artículo 35, intitulado: La Utilización de la Informática (*Utilizaçâo da informática),* en el contexto de los ADereitos e Deveres fundamentais@ (Parte I), y más concretamente en el Capítulo I, de los ADereitos,

liberdades e garantías pessoais@. Se establece así una inequívoca institucionalización del derecho de *habeas data* como una garantía cautelar de protección del conjunto de derechos y libertades fundamentales, y por supuesto del derecho de la intimidad (art.14).

El derecho de control a la información de uno mismo, constitucionalmente amplia su ámbito garantísta de los derechos y libertades fundamentales en la Constitución Portuguesa de 1976, cuando expresamente sostiene: A*Todos los ciudadanos tienen derecho a tomar conocimiento de lo que consta en forma de registros informáticos que les conciernen y de la finalidad a la que se destinan esas informaciones (datos o registros), y podrá exigir, llegado el caso, la rectificación de los datos, así como su actualización* (art.35-1).--Inconcebiblemente, López Díaz, traduce Aregistros informáticos@ como Aregistros mecanográficos@ [**123**]--. Entonces, el texto constitucional, prevé además del conocimiento previo exacto, claro e inequívoco de una información personal que le concierne a un individuo, los derechos, según fuere el caso, de rectificación y actualización de la información.

Conjuntamente con la constitucionalización del derecho de *habeas data* para la protección del conjunto de derechos y libertades fundamentales, la Constitución Portuguesa, plasma una serie de parámetros sobre el tema y sobre la regulación del

---

(123) LOPEZ DIAZ, E. Ob. cit., pág. 241

tratamiento informático de datos, lo cuales posteriormente serán objeto de reglamentación en la Ley de Agosto 20 de 1992. Estos son: a) La interdicción al acceso de terceros a los ficheros (o banco de datos) que contengan datos personales o a la respectiva interconexión de aquéllos, a través de los flujos transfronterizos, salvo en las casos exceptuados en la ley (art. 35-2); b) La informática no podrá ser utilizada para el tratamiento de datos referentes a las convicciones filosóficas o políticas, a la filiación partidista o sindical, a la fe religiosa o la vida privada, salvo cuando se trata de procesamiento de datos no identificables individualmente para

fines estadísticos.(art.35-3); y, c) Los registros informáticos serán regulados mediante ley; y, c) Se prohíbe la atribución de un número nacional único a los ciudadanos. **[124]**

En el derecho Español, la regulación constitucional del derecho de *habeas data* es orden constitucional (art. 18.4 y art.105-b, CE) y de ámbito legislativo interno por legislación especial sobre la materia: La LORTAD de 1992 y Ley de Régimen Jurídico de las Administraciones Públicas y procedimiento administrativo Común, LRJAP, L.O. 30 de Nov.27 de 1995); así como, por incorporación al ordenamiento jurídico interno del Convenio 108/1981, mediante instrumento jurídico idóneo ratificado y publicado en el BOE (Nov.15/1985. Art. 96.1 CE), como le sucedió con el Convenio Europeo de Estrasburgo de 1981, de 28 de Enero sobre el Atratamiento automatizado de datos de carácter personal@; o por transposición de las normas comunitarias sobre el particular de la Directiva 95/46/CE.

En el derecho Colombiano, el derecho de *habeas data*, como se dijo tiene una regulación preconstitucional a nivel legislativo en la Ley 16 de 1976, arts. 13 y 14, el C.C.A. (Dec.01/84-89) y en la Ley 57 de 1985, básicamente. En el art. 15 de la Constitución de 1991, se lee:

> ATodos...tienen...derecho a su intimidad...*Del igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas.... En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución...*@

---

(124) Texto completo de la Constitución Portuguesa de 1976, reformada en 1992, particular el art. 35, en: AA.VV. *CONSTITUÇAO NOVO TEXTO*. Coimbra editora, Ediçao organizado JJ. Gomes Conotilho o vital Moreira, 1982

Este art. 15 complementado por el art. 20 y 74, regula en forma expresa, amplia y con evidente falta de técnica codificadora, el derecho de *habeas data*, vez que constitucionaliza las etapas del procedimiento o tratamiento informático de la información o datos de carácter particular. En éste último aspecto la Constitución

Colombiana junto a la Portuguesa de 1976, quizá sean las únicas que haya constitucionalizado materias que son más de resorte y ámbito legal.

La falta de técnica de codificación del derecho de *habeas data*, por parte del Constituyente Colombiano de 1990, se observa al incorporar a renglón seguido (ADel igual modo,...@) y dentro del contexto de los derechos de Ala intimidad personal y familiar@ y el derecho Aal buen nombre@, el derecho de habeas data, tal como si fuesen uno solo e indisoluble, y no como lo que son: Aderechos autónomos y fundamentales@ (CC., Sent. T-097, de 3 de Marzo), y como tal codificables en artículos separados, tal como se procedió en la Constitución Portuguesa, al contextuarlos en el Capítulo de derechos y libertades fundamentales y establecer que el derecho de habeas data es un derecho que garantiza y protege el conjunto de derechos y libertades fundamentales, y no única y exclusivamente el de intimidad y el buen nombre.

El habeas data al igual que el *habeas corpus* no garantías exclusivas y excluyentes de ciertos derechos y libertades, ni tampoco puede explicarse la existencia de uno con la del otro, a tal punto de fusionarlo en uno sólo, el llamado derecho a A*libertad informática*@, tal como sostuviera *Frossini*, según lo comenta *Londoño* [125]

---

(125) ASi comparamos el derecho al *Habeas Data* con el de la intimidad y la información podemos concluir: Frente al derecho a la información: es un derecho moderno que se convierte en un limite que se le pone al derecho de información. EI Habeas Data limita el derecho a la información, determina hasta donde Ilega el deber de quien pretende informar y que es lo que puede exigir quien es objeto de esa información o quien la recibe. Frente al derecho a la intimidad: para algunos autores como Frossini este derecho es una extensión, es el concepto actual del Right of Privacy o Derecho a la Privacidad, estos autores consideran el Habeas Data estrechamente ligado a la intimidad pero con un contenido mas acorde a la realidad. Actualmente muchos doctrinantes le dan un carácter autónomo a este derecho, también reconocen que depende en gran medida del derecho a la intimidad, pero, creen que su contenido permite considerar que es un derecho fundamental moderno y autónomo@ . El derecho de Habeas data Aes el resultado del desarrollo de la tecnología informática y pretende solucionar el conflicto generado por la violación de los derechos a la intimidad y a la información y el conflicto que entre ellos se ha ocasionado. Es un derecho moderno, reciente y en inminente evolución. La denominación aun no ha sido unánime, para algunos es "el derecho a la protección de datos", otros lo Ilaman "*libertad informática*" (*V.Frossini:* ALa protección de la Intimidad: De la Libertad Informática, al Bien Jurídico Informático")., "Habeas Scriptum" (*Truyol y Serra*) y últimamente Habeas Data@. LONDOÑO TORO, Beatriz. DERECHO A LA INTIMIDAD Y BANCOS DE DATOS FINANCIEROS. ANALISIS DOCTRINAL Y JURISPRUDENCIAL. *En: INFORMATICA JURIDICA Y DERECHO INFORMATICO*. Ed. Señal, s/n, Medellín (Col.)

y alguna jurisprudencia de la Corte Constitucional [126]. Estas posturas giran en la tónica interpretativa de identificar el derecho de habeas data con el derecho a la intimidad, cuando la información o datos personales se han sometido a tratamiento (recolección, almacenamiento, conservación, registro y transmisión) informatizado y cuando se ha producido el desconocimiento, vulneración, quebranto o negación de una cualesquiera de las facultades inherentes del habeas data (acceso, actualización, rectificación y cancelación de la información o datos).

Sin embargo, en las Sentencias de Unificación de criterios y jurisprudencia de la Corte Constitucional (SU-082 y SU-089 de Marzo 1 de 1995), se ha individualizado plenamente los derechos de *habeas data* y a la intimidad. En los fructíferos como reiterados pronunciamiento de la Corte, se ha establecido que el derecho fundamental y autónomo de habeas data está instituido en la Constitución, además, como un derecho que garantiza la protección del conjunto de derechos y libertades fundamentales. Así, a título de ejemplo, enunciemos algunos: El derecho a la intimidad de las personas naturales o físicas (CC., Sent.022/1993, de 29 de Enero), la intimidad de las personas jurídicas (CC., Sent.T-462/1997,de 24 de Sep.), el derecho al buen nombre, el derecho a Ala honra@ (CC .Sent T-413/1993, de 29 de Sep., CC., Sent. T-097, de 3 de Marzo), el derecho al libre desarrollo de la personalidad (CC. Sent. T-542/1992, de 25 de Sep., T-493, de 28 de Oct., [127] y la Sent. 549/1993, de 15 de Dic., Acambio de nombre@); entre

---

(126) AEl derecho a la intimidad comprende varias dimensiones de la vida privada. En este caso concreto, sin embargo, se trata sólo de una de tales dimensiones: el habeas data...@ (Corte.Cons. --CC--. Sent T-444/1992, Julio 7)

(127) Corte Constitucional Colombiana: *A- Sent. T-542, de 25 de Sep*., desentraña el origen y antecedente del art. 16 de la Cons. Col., sobre el derecho al desarrollo de la personalidad o Aderecho a la autonomía personal@, en los siguientes términos: este derecho A en el informe ponencia para primer debate en plenaria en la *Asamblea Nacional Constituyente*, se estableció: "En la época actual, el desarrollo de la personalidad no sólo tiene trabas y obstáculos que se conocieron en otros tiempos, sino que el individuo pretende ser condicionado a través de *sofisticados medios tecnológicos* (Se refiere a los nuevos fenómenos tecnológicos TIC y la informática, electrónica y telemática) que han permitido a algunos sociólogos identificar el fenómeno como de alienación. Tal circunstancia llevó a los miembros de la Comisión Primera a consagrar el derecho a la autonomía personal, sin otras limitaciones que las que imponen el respeto a los derechos de los demás y al orden jurídico. El riesgo de manipulación cultural, no deja de ser una de las graves amenazas para que el individuo desenvuelva cabalmente sus potencialidades intelectivas, y tal es el sentido del artículo que se propone introducir en la Constitución nacional". El artículo 16 de la Constitución Política establece: "Todas las personas tienen derecho al libre desarrollo sin más limitaciones que las que imponen los derechos de los demás y el ordenamiento jurídico". *B.*-

La Sent. T-493/93, Oct. 28, establece el contenido esencial de este derecho y su entronque con el derecho a la intimidad, en los siguientes términos: A El derecho al libre desarrollo de la personalidad consiste en la libertad general, que en aras de su plena realización humana, tiene toda persona para actuar o no actuar según su arbitrio, es decir, para adoptar la forma y desarrollo de vida que más se ajuste a sus ideas, sentimientos, tendencias y aspiraciones, sin más restricciones que las que imponen los derechos ajenos y el ordenamiento jurídico. El derecho al libre desarrollo o desenvolvimiento de la personalidad, o de libertad de opción y de toma de decisiones de la persona, ejercido dentro del marco del respeto de los derechos de los demás y el orden jurídico, es un derecho
otros derechos fundamentales.

El derecho de habeas data, en el derecho colombiano, tiene como sujeto activo a Atoda persona física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado. El sujeto pasivo es toda persona física o jurídica que utilice sistemas informáticos para (la recolección, almacenamiento, registro), la conservación, uso y circulación de datos personales@--paréntesis nuestros-- (CC., Sent. SU-082/1995, Fundamento Jurídico No.5).

AEl contenido del derecho de habeas se manifiesta por tres facultades concretas que el ... artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados: a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día agregándoles los hechos nuevos; y c) El derecho a rectificar las informaciones que no correspondan a la verdad... y el *derecho a la caducidad del dato negativo* @ (CC., Sent. SU-082/1995, F.J.5), tanto de las informaciones falsas, erróneas, o Aen el caso de las verdaderas, lo sigue haciendo (se refiere a la afección a los derechos del titular) no obstante haber caducado el dato...@ APues, el ejercicio de este derecho (a la caducidad, se refiere) no corresponde a una sanción,... esta sustentado en el art.20 (derecho a recibir información veraz) de la Constitución... (Por tanto). El *derecho al olvido* (CC.,Sent.414/1992, de 6 de Junio)... las informaciones negativas acerca de una persona no tienen vocación de perennidad y en consecuencia, después de algún tiempo, deben desaparecer totalmente del banco de datos respectivo@ --paréntesis nuestros-- (CC., Sent. 097/1995, de 3 de Marzo).

Este desaparecimiento del dato, registro o información codificada, por caducidad

---**Continuación Nota 127**---
constitucional fundamental, pues no sólo así se encuentra consagrado en el artículo 16 de la Constitución Nacional, el cual hace parte del capitulo 1 del titulo II, denominado "De los derechos fundamentales", sino que esa connotación le ha sido reconocida por esta Corporación, entre otras, en las providencias T-050 del 15 de febrero de 1993 y C-176 del 6 de mayo de 1993. (F.J. 5.1)@. ALa violación del derecho al libre desarrollo de la personalidad, implica el quebrantamiento del derecho a la intimidad,.... Si el derecho al libre desarrollo de la personalidad es concebido como la libertad individual de toda persona para tomar por sí sola decisiones que conciernen a la esfera de su vida privada, es evidente que los atentados contra aquel derecho, en casos como el sub examine, pueden afectar el derecho a la intimidad. (F.J. 5.2.)@ Textos completo en: *WWW. RDH. GOV. CO.* 1998.

o por cualquier otra causa prevista en el ordenamiento jurídico vigente, constituye la condición *sine qua nom* de la cancelación o la supresión (o en términos informáticos ABorrado@ o Aeliminación@), o del bloqueo (con carácter cautelar hasta cuando cesen las causas que lo originaron) de la información contenida en una base de datos, constituyen dos de las facultades últimas e inherentes al derecho de *habeas data*.

3.4. El Derecho de información previa y el derecho de AOposición@ al tratamiento informático:

Estos dos derechos completan el cuadro de la compleja visión iusinformática de los derechos y libertades fundamentales, y en particular, la del derecho de la intimidad.

3.4.1. Derecho a la información, cuando los datos personales han sido recabados o no del propio interesado.

El derecho de información previa del titular de los datos personales que le conciernen se halla establecido en el art. 5-1, complementado y ampliado en sus efectos a todo el procedimiento o tratamiento informatizado por el art. 13 de la LORTAD. Este derecho subjetivo del concernido consiste en Aser previamente informado de modo expreso, preciso e inequívoco@, de todo cuanto sea necesario, en el momento en que sean solicitados datos a él referidos, y por su puesto, vayan a ser objeto de recolección y posterior almacenamiento, registro, conservación e incluso transmisión por medios informáticos, electrónicos o telemáticos, por quienes así proceden (sean personas naturales, jurídicas, públicas o privadas).

El concernido puede ser informado previo a cualquier tratamiento informatizado de datos personales, sobre aspectos tales como: la existencia de una base de datos de carácter, la finalidad que persigue la recolección de la información personal y los destinatarios; el carácter facultativo u obligatorio de las respuestas o preguntas que se le plantean; la consecuencia de la obtención de los datos o de la negativa a suministrarlos, etc.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, regula el derecho de información previa al tratamiento informatizado de datos personales, en forma diversa si los datos son recabados del propio interesado (art.10), o cuando no se han hecho de esta forma (art.11).

En efecto, si los datos han sido recogidos del propio interesado, los Estados Miembros de la UE, en sus diferentes regulaciones normativas sobre el particular, deberán disponer que el responsable del tratamiento o su representante deban comunicar a la persona concernida con los datos, al menos lo siguiente: a) la identidad del responsable del tratamiento o su representante, b) los fines del tratamiento de que va a ser objeto los datos, c) los destinatarios o categorías de destinatarios de los datos, d) el carácter obligatorio o no de las respuestas y las consecuencias que tendría la persona a la negativa a responder, e) la existencia del derecho de acceso y rectificación de los datos que le conciernen.

Si los datos no han sido recolectados del propio interesado, los Estados Miembros de la UE, dispondrán que el responsable del tratamiento o su representante, desde el momento del registro de los datos, o en el caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al menos, idéntica información a la relatada anteriormente para el caso de haber sido recaba la información del propio interesado, salvo que éste ya hubiera sido informado sobre ello.

La diferencia entre un sistema y otro de ejercicio del derecho de información previa, estriba no sólo en el momento, etapa o fase del procedimiento informatizado (la recolección, para el caso previsto en el art.10, y la fase de registro, para el evento del art. 11), sino en cuanto a que, en el último caso, la información pertinente que se debe dar al interesado del cual no se ha recabado la información, no será necesaria, cuando el tratamiento informatizado se aplique Acon fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley@. Estas causales de excepción, al principio de información previa, tienen algunas un cierto grado de subjetividad o discrecionalidad por parte de los funcionarios o personas que deben aplicarlas, sin embargo, como facultad discrecional no implica arbitrariedad, la Directiva establece límites a esa discrecionalidad, al exigir que los Estados Miembros de la UE, Aestablecerán las garantías apropiadas@ (art. 11-2 *In fine*) para regular estas excepciones. (Directiva 95/46/CE).

3.4.2. El derecho de oposición al tratamiento informatizado de datos.

Este *novo* derecho constituye una garantía de protección máxima a los titulares de los datos personales que van a ser sometidos a tratamiento informatizado. Esta prevista en la Directiva 95/46/CE [128].

El derecho de oposición al tratamiento de datos, se manifiesta de dos formas: a) Como derecho de oposición al tratamiento propiamente dicho (art. 14); y, b) Como derecho de una persona a no verse sometido a una decisión individual informatizada con efectos jurídicos sobre aquélla (art. 15).

El derecho de oposición del interesado, se ejercita por el interesado en cualquier momento del tratamiento de datos y Apor razones legítimas propias de su situación particular@ (o motivos fundados y legítimos relativos a su situación concreta, según se explica en el C.45), frente al tratamiento de cualquier dato personal que le concierna. Al final de este aparte, comentaremos este derecho a profundidad.

Sin embargo, como sostienen *Dumortier y Alonso Blas* [1 29], la efectividad del derecho de oposición (en sus dos vertientes, agregamos) exige que se concrete un procedimiento de tutela del mismo, así como la inclusión de la tipificación de las conductas que el son contrarias, así como la correspondiente sanción.

Este derecho de oposición al tratamiento informatizado todavía no ha sido incorporado al ordenamiento jurídico interno Español, pese a que la transposición normativa de la Directiva, temporalmente se cumple el 28 de Octubre de 1998.

---

(128) Considerandos --en adelante C.-- núms. 25 y 30., conc., art. 14 y 15 Directiva. Texto completo en: WWW.CC.CEC. (Base de datos de la Unión Europea. Bruselas).1997.

(129 DUMORTIER, J. Y ALONSO BLAS, Diana. *LA TRANSPOSICION DE LA DIR*ECTIVA DE PROTECCION DE DATOS. En: Actualidad informática Aranzadi. Ed. Aranzadi S.A., A.I.A. Núm. 20 de Julio., Pamplona, 1996, 1 y ss.

4. ORDENAMIENTOS JURIDICOS DE PROTECCION Y GARANTIA DE LA VISION IUSINFORMATICA DE LA INTIMIDAD, A TRAVÉS DE LAS LEYES DE PROTECCION DE DATOS PERSONALES.

4.1. PRELIMINARES.

Nos parece oportuno en esta parte del trabajo, hacer mención a los diferentes cuerpos normativos que regulan el tratamiento informatizado de los datos de carácter personal, a efectos de exaltar, entre otros aspectos, por un lado, la labor que vienen cumpliendo los legisladores en los diferentes Estados del mundo por puntualizar y establecer un marco de garantías y medias de protección a los derechos involucrados en dicho tratamiento (derechos a la información, expresión, habeas data, honor, imagen, intimidad, etc); y por otro, analizar, estudiar y puntualizar la *visión*

iusinformática del derecho a la intimidad, prevista en las principales leyes de protección de datos personales, clasificadas inicialmente en *tres generaciones*, según sus contenidos y evolución en la regulación del fenómeno informático en entronque con el derecho. Ampliaremos luego una cuarta generación y otra en transición, atendiendo además de lo dicho, al factor temporal, los avances significativos de iusinformática y la consideración de los Estados Aparaísos informáticos@ técnica como legislativamente.

En la *primera generación* de estas leyes se hallan las denominadas *leyes pioneras* en la regulación y tratamiento (informatizado o no) de datos de carácter personal: La *LEY FEDERAL ALEMANA DE PROTECCION DE DATOS PERSONALES* y Ley Sueca A*Data lag@* de 11 de mayo de 1973 [130] . Según *Mirabelli* [131] , estas leyes son tendencialmente restrictivas puesto que se sujetan al requisito de Ala autorización previa@ para la creación de los *Aficheros@* o bancos de datos, limitando excesivamente la recolección de los Adatos sensibles@ e instituyendo organismos con funciones y estruc-

---

(130) La Data lag Sueca, según el profesor ORTI, Aestableció un sistema de Registro de ficheros informatizados, exigiéndose la inscripción con carácter constitutivo, necesaria para obtener la autorización para crear un fi- chero, y a la que se condicionaba la inclusión en el Registro. Este requisito fue sustituido más tarde por el sistema de la mera notificación e inscripción registral, que es el seguido en la ley española@ Cfr ORTI VALLEJO, Antonio. *DERECHO A LA INTIMIDAD E INFORMATICA (Tutela de la persona por el uso de ficheros y tratamiento informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*. Ed. Comares, Peligros (Granada), 1994, pág.14.

(131) MIRABELLI, *ABanche dati e contemperamento degli interessi@, Bance dati telematica e diritti della per- sona*, Cedam, Padova, 1984, pág. 160. Citado por ORTI V. Ob. cit., pág. 11.

tura cuasi jurisdiccional para la concesión y el ejercicio del control de los mencionados banco de datos [132]. Sin embargo, como veremos más adelante la Ley Alemana, --que tomamos como prototipo de análisis de esta primera generación-- por contra, se caracteriza por ser la primera en el tratamiento integral de tratamiento informatizado o no de datos personales, así como de demarcar una nueva técnica legislativa en materia de definiciones técnico-jurídicas, estructurar por vez primera los Aprocesos de datos@ públicos y privados y crear la figura del Comisario de Protección de datos para la vigilancia, garantía y protección de los derechos fundamentales, las libertades públicas e intereses legítimos de los titulares

de datos personales. Temas que se tratarán brevemente, pues sirven a los propósitos iniciales y finales de la investigación.

En una *segunda generación de leyes* protectoras de los datos personales se destacan la de Francia en 1974, Noruega en 1978, Luxemburgo en 1981, etc. Por paralelo y con idénticos propósitos, surgen normas de ámbito internacional (La Recomendación de la OCDE de 1980) y Comunitario Europeo propuestas por el Consejo de Europa (El Convenio de Estrasburgo de 1981). Las leyes en esta etapa se caracterizan por el sistema de Ala notificación@ y no de la autorización como requisito *a priori* para crear bancos de datos [133], se ingresa en la técnica legislativa de la conceptualización de los términos técnico cerrados y abiertos utilizados en las nuevas tecnologías de la información y la comunicación (TIC) que inciden en el derecho y se instituye, a partir de éstas, los denominados Aprincipios fundamentales de la protección de datos@, tanto en el tratamiento, almacenamiento, difusión como en la Alibre circulación de datos de carácter personal@. Aspectos capitales en el procedimiento informatizado de datos que se evidenciaron más en las normas de ámbito internacional y comunitario, antes que en las leyes estatales, como precisaremos.

---

(132) En ésta etapa de clasificación de normas de protección de datos personales, nacieron por doquier varias leyes en Europa y América.. Se destacan entre ellas la Ley Francesa de 6 de Enero de 1978, conocida como A*Loi relative à l´informatique, aux fichiers et aux libertés,* y la *Privacy act* de 31 de diciembre de 1974, que fueron el prototípo de otras que les siguieron . Entre ellas, la Ley Noruega de Junio 9 de 1978, la de Luxemburgo de 30 de Marzo de 1979, la Suiza de 1981.

(133) Ob. ut supra cit. pág. 11.

Por ello, tomaremos de ésta generación dos prototipos de legislación sobre el tratamiento informatizado de datos: La Recomendación del Consejo de la OCDE de Septiembre 30 de 1980, *por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales* y El Convenio Europeo de Estrasburgo de 28 de Enero de 1981", relativo a la *Aprotección de las personas con respecto al tratamiento automatizado*

de datos de carácter personal@. Convenio incorporado por todos los Estados Europeos en sus respectivos ordenamientos jurídicos internos a través de normas jurídicas de trasposición. En España, el Convenio se ratificó mediante instrumento de Enero 27 de 1984 (BOE. 15-11-1985, núm. 274) e ingresó al ordenamiento jurídico interno no sólo como mecanismo de interpretación de derechos humanos (art.10.2 CE), sino como una verdadera norma jurídica con fuerza legislativa desde aquélla época (art.96.1 CE).

En la A*tercera generación@*, se ubican las normas jurídicas nacidas en la década de los noventa, muy a pesar de que las propuestas e iniciativas venían manejándose desde la década anterior. En esta se ubican la *ALa ley española de regulación del tratamiento automatizado de datos de carácter personal@*, de 29 de Octubre de 1992, conocida también como LORTAD, como también la *APrivacy and data Protection Bill 1994 (NSW) o Ley de protección de la intimidad y los datos personales en Australia.* Esta generación de leyes se caracteriza según *Orti Vallejo* [134], siguiendo a *Pérez Luño*, por ser más Aliberalizantes del uso de ficheros de datos personales@ y establecer un amplio marco de principios, derechos y obligaciones para las personas naturales, jurídicas, públicas y privadas.

Una *cuarta generación* de normas surge con la expedición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.* Esta generación se caracteriza por plantear como epicentro el principio-derecho de la libre circulación de datos personales
entre los países miembros de la Unión Europea e incluso entre países terceros, previo el lleno de unos requisitos *sine qua nom;* la consagración de principios, derechos (como
el de información y de habeas data) y obligaciones en todas las fases, etapas o ciclos

---

(134) ORTI VALLEJO, A. Ob. cit.. pág. 18

informáticos del procedimiento informatizado de datos, cuando se realiza con soportes, medios y aplicaciones informáticas, electrónicas y telemáticas [135] y la plasmación del llamado *derecho de oposición al tratamiento informatizado* de datos personales, como un derecho personalísimo de los titulares de los datos personales.

Finalmente, una *quinta generación* o *generación de leyes protectoras de datos específicas en tránsito*, constituida por Estados que no disponen de normas especiales en la protección de datos personales, pero en cambio disponen de diversas normas jurídicas generales, mecanismos y procedimientos jurisdiccionales de índole constitu- cional, contencioso-administrativo, civil y penal. Igualmente, disponen de recursos en Avía administrativa@ contra las decisiones, actos u operaciones del Estado y normas que regulan aspectos puntuales (v.gr.El derecho a la información, habeas data, etc), pero no integrales del tratamiento informatizado de datos personales. En todo caso, estos Estados con este conjunto de normas e instituciones jurídicas, propenden por la efectiva protección de los derechos y libertades fundamentales, en todos los ámbitos incluidos aquellos que se presentan en el tratamiento informatizado de datos. Quizá por ello, en puridad no existen *AEstados paraísos informáticos*@por el sólo hecho de no tener normas superespecíficas en algunas materias que develan la tensión-relación de la informática con los derechos humanos, pues estas están inmersas en una amplia gama de protección general de los derechos fundamentales que todo Estado dispone. En el derecho Colom- biano, se dispone de una regulación constitucional específica de los derechos fundamentales de la intimidad, del habeas data, del libre desarrollo de la personalidad, de la información y de expresión (arts.15, 16,20,73,74 Cons.Pol.), así como un ordenamiento jurídico que desarrolla el derecho de la información y el habeas data (Ley 57/1985, C.C.A de 1984/1989, etc) como mecanismos coadyuvantes de protección de los derechos fundamentales, entre ellos el de la intimidad, cuando se esta ante procedimientos de datos informatizados o no. Así mismo se cuenta con una amplia, fruc tífera y puntual jurisprudencia de la Corte Constitucional,@salvaguarda de la Constitu- ción@, la cual va desentrañado la visión iusinformática del derecho a la intimidad en sus decisiones de protección del derecho de la intimidad, información y habeas data (C.C. Sents.T-414/ 1992, Ago.T-444/92 de 7Jul. T-

127/1994, de 15 de Mar.), derecho de ha- beas data (CC. T-022/1993, de 29 Ene.), el derecho al buen nombre (C.C. Sent. T-413/

---

(135) Véase, parte III, punto 5 y ss.

1993, de 29 de Sep.), derecho a la información, la intimidad y el habeas data (CC.Sent. T-097/1995, de 3 de Mar. Sent SU-082 y 089/1995, de 1 de Marz.), el derecho de Aautodeterminación informática@ (C.C. Sent.T-552/1997, de 30 de Oct), etc.

Veamos ahora, las normas prototipo de cada generación.

4.2. ALEMANIA: LA LEY FEDERAL DE PROTECCION DE DATOS DE 27 DE ENERO DE 1977 [136].

Esta Ley Federal es el resultado de la estructuración y promulgación de la Ley perteneciente al *Land de Hesse* de 7 de Octubre de 1970, primera en regular todo lo atinente al tratamiento informatizado de datos que Autilizaban los servicios administrativos del Land@ y de la ley de la Renania-Palatinado [137]

La Ley Federal de protección de datos, no sólo fue la pionera a nivel internacional en regular legislativamente el tratamiento informatizado de los datos personales, sino que es la primera y la única, incluso hasta épocas actuales, en tratar integralmente todo lo atinente al tratamiento informatizado los datos personales, tanto en el ámbito público como privado; así como también en regular los aspectos civiles, penales y derecho público derivados del ejercicio, protección y transgresión de los derechos que ostentan los titulares de los datos, ante las autoridades civiles, administrativas y punitivas.

La Ley Federal Alemana de protección de los titulares de los datos, el 20 de diciembre de 1990, recibió una nueva redacción en su texto y que en esencia su contenido y su Aconcepción sigue siendo igual a la de 1997" [138] . Por ello,

estudiaremos brevemente el texto de 1977. Esta ley (en adelante LFAPD), tiene cinco secciones de las que destacaremos los aspectos que tienen que ver con el objeto de nuestro trabajo. Son:

SECCION PRIMERA: Disposiciones generales: En las que se refiere a los co-

---

(136) Texto completo en AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla. Tratados Inter. núm.2.
(137) ORTI VALLEJO, A. Ob. cit. pág. 12
(138) Según Heredero Higueras, citado por ORTI VALLEJO, Ob. ut supra cit., pág. 12-13.

metidos y objeto de la ley, definiciones, admisibilidad del Aproceso de datos@, derechos del Aafectado@; y, Asecreto de los datos, medidas técnicas y de organización@.

SECCION SEGUNDA: Proceso de datos de autoridades y otros servicios públicos: ámbito de aplicación; elaboración de datos personales por cuenta ajena; almacenamiento y modificación de datos; comunicación de datos dentro del sector público; comunicación de datos a Aentes@ ajenos a un sector público; Publicidad de los datos almacenados; Facilitación de información Aal afectado@; Rectificación, bloqueo y cancelación de datos; Ejecución de la protección de datos en la Administración Federal; Disposiciones administrativos de carácter general; nombramiento de un Comisario Federal de Protección de datos; situación jurídica del Comisario Federal de Protección de Datos; Funciones del Comisario Federal de Protección de Datos; Reclamaciones del Comisario Federal de Protección de Datos; y , Recurso ante el Comisario Federal de Protección de Datos.

SECCION TERCERA: Proceso de datos de entes no público para uso interno: Ambito de aplicación; modificación de datos; facilitación de información al afectado; Rectificación, bloqueo y cancelación de datos; Designación de un Comisario de Protección de Datos; Funciones del Comisario de Protección de Datos; y, Autoridad de tutela.

SECCION CUARTA: Proceso de datos realizado con finalidad mercantil para entes no públicos: Ambito de aplicación; Almacenamiento y comunicación de datos; modificación de datos; facilitación de información al Aafectado@; Rectificación, bloqueo y cancelación de datos; elaboración de datos personales para su difusión en forma Aanonimizada@ (o simplemente anónima); elaboración de datos personales por cuenta ajena; Comisario de Protección de Datos; Deber de denuncia; y, Autoridad de tutela.

SECCION QUINTA: Normas punitivas y sancionadoras: Acciones punibles, y, Infracciones de Policía.

SECCION SEXTA: Disposiciones transitorias y finales: Disposiciones finales; Aplicación de la Ley de Procedimiento Administrativo; Disposiciones subsistentes; ACláusula Berlinesa@; y , entrada en vigor.

Son muchos y variados los temas los que aborda la Ley alemana, sin embargo, destacaremos a nuestros efectos investigativos los siguientes, los cuales los dividiremos así: a) Las definiciones técnico-jurídicas iusinformáticas; b) El Comisario de Protección de los Datos; y c) El Sistema Punitivo y Sancionador en materia de datos.

4.2.1. DEFINICIONES TECNICO-JURIDICAS IUSINFORMATICAS.

La Ley Federal Alemana del tratamiento de datos personales, inaugura en su condición de pionera, la técnica legislativa que posteriormente se extendiera en toda norma jurídica estatal y comunitaria de iniciar el texto legislativo con un glosario de términos técnico-jurídicos cerrados, cuyas definiciones son de aplicación necesaria para todo operador jurídico de la ley. Las definiciones contenidas en la Ley de 27 de Enero de 1977, son *iusinformáticas*, por referirse a la órbita jurídica tanto al derecho público como al derecho privado y en particular, al tratamiento informatizado de datos dominado por la informática.

Las diversas definiciones las podemos agrupar por su contenido y afinidad con el fenómeno tecnológico de la informática (entendida como la ciencia del tratamiento lógico, sistematizado e informatizado de cualquier unidad de información o datos) y el derecho, en los siguientes: a) Definiciones sobre los sujetos del tratamiento de datos; b) Definiciones aplicables al A*Habeas Data*@ y al proceso de datos personales; y, c) Definiciones aplicables al procedimiento informatizado de datos.

4.2.1.1. DEFINICIONES SOBRE LOS SUJETOS DEL TRATAMIENTO DE DATOS.

Pertenecen a este grupo las definiciones de ADatos personales@, Atercero@y Aente almacenante@. *Datos personales* se consideran las indicaciones concretas acerca de condiciones personales o materiales de una persona natural determinable (o Aafectado@, aunque en puridad sería el interesado o titular de los datos). Estos datos personales como información perteneciente a cualquier persona física, incluye tanto la contenida en método no informáticos, como en aquellos a los que se les ha aplicado la técnica, tratamiento o procedimientos informatizados o A*procedimientos automáticos*@, como lo denomina la Ley Federal Alemana de Protección de Datos. Se excluyen no del concepto de datos personales sino del ámbito de aplicación de la LFAPD, los datos personales elaborados por empresas auxiliares de la prensa, radio o cinematografía, exclusivamente para uso interno en relación con la difusión (Art. 1 *in fine* LFAPD), salvo en lo atinente a las Amedidas técnicas y de organización@ que éstas deben implementar para garantizar los derechos e intereses legítimos de los titulares de los datos de conformidad con LFAPD [139].

Tercero, es toda aquella persona o entidad (Aente@) ajena a la entidad almacenante, a excepción de los interesados o de aquellas personas y entidades (Autoridades públicas, personas jurídicas, sociedades u otras agrupaciones, etc) que obraren por Aencargo@ dentro del ámbito de vigencia de la LFAPD.

Y, finalmente, *Entidad Almacenante*, se consideran como tales cualquiera de las personas naturales o jurídicas o entidades que almacenaren datos por sí mismo o enco-

---

(139) ASi se elaboraren automáticamente datos personales, deberá adoptarse para la aplicación de los preceptos de la presente ley medidas que en función de la índole de los datos personales que hubieren de ser protegidos fueren idóneas para: l. impedir a personas no autorizadas el acceso a los equipos de proceso de datos con los cuales fueren elaborados los datos personales (control de acceso a los equipos); 2. impedir que las personas ocupadas en la elaboración de datos personales retiren sin autorización soportes de información (control de salidas); 3. impedir la introducción no autorizada en memoria de datos personales, así como la toma de conocimiento, modificación o cancelación no autorizadas de datos personales ya almacenados (control de memorias); 4. impedir que personas no autorizadas utilicen sistemas de proceso de datos a partir de los cuales se comunicaren datos personales valiendose de dispositivos automáticos o en los cuales se introdujeren datos personales valiendose tales dispositivos (control de usuarios); 5. garantizar que las personas con derecho a usar un sistema de proceso de datos puedan acceder mediante dispositivos automáticos exclusivamente a los datos personales que estuvieren comprendidos dentro del ámbito de su facultad de acceso (control de acceso a los datos) ; 6. garantizar que se pueda comprobar y determinar en que puntos es posible comunicar datos personales valiendose de dispositivos automáticos (control de la comunicación); 7. garantizar que se pueda comprobar y determinar a posteriori que datos personales, en que momento y por quien fueron introducidos en sistemas de proceso de datos (control de la introducción en memoria); 8. garantizar que en los datos personales que fueren elaborados por cuenta ajena sólo puedan serlo de conformidad con las instrucciones del comitente (control de encargos); 9. garantizar que en los supuestos de comunicación de datos personales, así como en los casos de transporte de los correspondientes soportes de información, estos no puedan ser leídos, modificados o cancelados sin autorización (control del transporte de datos); 10. configurar la organización interna de las autoridades o empresas de tal manera que la misma responda a las exigencias de la protección de datos (control de la organización)@. ANEXO AL ARTICULO 6, PRIMER PARRAFO, PROPOSICION PRIMERA.

comendare a otro su almacenamiento. Estas son: a) Las diversas Autoridades o entidades públicas (pertenecientes al Estado, a los Municipios, mancomunidades de municipios y cualquier otras personas jurídicas de derecho público sujetas a tutela estatal. Art. 7 LFAPD); y, b) Personas naturales o jurídicas, sociedades u otras agrupaciones de personas de derecho privado, para uso interno (se exceptúan de ésta aparte las personas de derecho privado que desempeñan Afunciones propias de la Administración Pública@. Art.22 LFAD), o las que realicen Acon carácter regular y por cuenta ajena@ actividades con Afinalidad mercantil@ (en esta se incluyen las empresas de derecho público, con idéntica finalidad. Art. 31 LFAPD).

4.2.1.2. DEFINICIONES APLICABLES AL AHABEAS DATA@ Y AL PROCESO DE DATOS PERSONALES.

Si bien como recuerda el profesor *González Navarro*, citando a *Heredero Higueras* [140], el derecho de acceso, aún antes de la promulgación de las leyes de protección de datos, fue bautizado como *habeas data*, por considerarlo como una modalidad de acción exhibitoria análoga a la del *habeas corpus* del derecho anglosajón, no debemos olvidar que el derecho de acceso a los datos, sobre todo los informatizados o sometidos en parte o en todo a tratamiento o procedimientos Aautomatizados@, conlleva un grupo de derechos concomitantes y subsiguientes al ejercicio del derecho de acceso, tales como: el derecho a conocer la existencia de datos que le conciernan a la persona y que se hallen almacenados (Astorage@) y contenidos en un fichero, banco de datos o simplemente en un AarchivoA o registro informatizado (o simplemente A*file*@ anglosajón), bien sean procesados con o sin su consentimiento; así como también el derecho a consultarlos, si fuere del caso, por cualquier método, técnica o medio informático, electrónico o telemático [141] , dentro de conformidad con el ordenamiento jurídico vigente sobre la materia. Como consecuencia, de ello podrá, independientemente de los recursos (básicamente jurisdiccionales), solicitar la revisión, rectificación, actualización, modificación y, llegado el caso, la cancelación, borrado y bloqueo de los datos persona-

---

(140) GONZALEZ NAVARRO, Francisco. *DERECHO ADMINISTRATIVO ESPAÑOL*. Ed. Eunsa, 1a., ed., 1987 y 2a., ed., 1994, Pamplona, pág. 179

(141) Véase, parte III y IV de esta investigación al respecto.

nales que le conciernan.

En consecuencia, pertenecen a este segundo grupo de definiciones, las siguientes:

almacenar, comunicar, modificar y cancelar datos personales.

Almacenar datos personales, en términos iusinformáticos, consiste en recoger, registrar o conservar en un soporte de información con miras a su ulterior utilización. El Aalmacenamiento@ de datos, según la LFAPD constituye una fase del procedimiento informatizado de datos que abarca una etapa previa, como es la recolección; una etapa concomitante, como es la del registro; y una etapa posterior,

como es la conservación de datos. Todas ellas interdependientes, pues faltando una de éstas no se puede completar el fenómeno o actividad de almacenamiento.

La LFAPD, establece la subsidiariedad de ésta, cuando existan leyes especiales federales sobre los datos personales almacenados en registros informatizados (art.45), destacando con ello la etapa de almacenamiento y tratamiento informatizado de los datos. Así a título de ejemplo, se aplicará la ley especial sobre la general en la guarda de secreto sobre noticias obtenidas oficialmente o en el ejercicio profesional; p. e., el art. 12 de la Ley de Estadísticas para fines Federales, de 3 de septiembre de 1953 [142].

La LFAPD, al hacer mención a los derechos que tiene el Aafectado@ (por titular de los datos, en términos positivos y no en términos negativos, tal y como lo prevé la ley) dentro del llamado Aproceso de datos@, se hace expresa referencia a los derechos derivados del acceso y consulta de la información y subsecuente, todos ellos componentes del derecho fundamental del *habeas data.* Los derechos subsecuentes son: a) La información acerca de los datos almacenados en relación con la persona; b) La Rec

---

(142) Otros ejemplos son: a) Sobre limitación del examen de documentos por terceros; p. e., el articulo 61, párrafo segundo y tercero de la ley de estado civil de las personas; b) Sobre examen del expediente personal por los funcionarios o empleados; p e., el articulo 90 de la ley federal de funcionarios; el articulo 83 de la ley de Organización de Empresas; c) Sobre el deber de las autoridades de informar a los ciudadanos de los datos almacenados acerca de los mismos; p. e., el articulo 1.325 de la Ordenanza Imperial del Seguro; g) Sobre difusión, rectificación y cancelación de los datos referidos a personas incluidos en Registros públicos; p. e., los artículos 19, 23, 27, segundo párrafo; y d) Sobre la obligación de elaborar datos referidos a personas en la rendición de cuentas, comprendidas la contabilidad y otras anotaciones; p.e., los artículos 38 a 40, 42 a 47 del Código de Comercio. Texto completo de la LFAPD., en AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla. Tratados Internacionales núm. 2

tificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; c) El bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y d) La cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien --a elección, ademas del derecho de

cancelación-- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

Comunicar, en términos de la LFAPD, es una especie cualificada (dirigida a Aterceros@) del género *informar* (que la ley denomina derecho de Afacilitación de in- formación al afectado@, considerado como un derecho fundamental, no absoluto que tiene el titular de los datos personales, tanto en el proceso de datos público [14 3], como en el privado [144], puesto que se prevé expresas excepciones al ejercicio del mismo), puesto
que comunicar se entiende la acción de dar a conocer a terceros datos almacenados u

---

(143) Se facilitará al afectado, si así lo solicitare, información acerca de los datos almacenados con relación a su persona. En la solicitud deberá detallarse la índole de los datos personales sobre los cuales deba facilitarse la información. El servicio o ente almacenante determinará el procedimiento, en especial la forma de facilitar información según las conveniencias del servicio... No precederá la facilitación de la información en los siguientes supuestos: 1. si la información perjudicare el legítimo cumplimiento de las tareas comprendidas en la competencia del servicio almacenante; 2. si la información perjudicare a la seguridad o al orden públicos o causare detrimento a la Federación o a un Estado; 3. si los datos personales o el hecho de su almacenamiento hubieren de ser mantenidos en secreto en virtud de norma jurídica o por razón de su esencia, en especial en razón del interés legítimo preponderante de un tercero ; 4. si la información hiciere referencia a la comunicación de datos personales a las autoridades mencionadas en el articulo 12, segundo párrafo, apartado 1. La facilitación de la información estará sujeta al devengo de una tasa... (art. 13 LFAPD).

(144) Si se almacenaren por primera vez datos referentes a la persona del afectado, deberá este ser informado de ello, a menos que hubiera tenido conocimiento del almacenamiento por otros medios. El afectado podrá e- xigir información acerca de los datos almacenados con relación a su persona. Si los datos fueren objeto de tratamiento automático, el afectado podrá exigir asimismo información acerca de las personas y servicios a los cuales fueren transmitidos regularmente sus datos. Deberá señalar la clase de los datos personales sobre los cuales debiere ser facilitada la información. La información se facilitara por escrito, siempre que no procediere otra forma de facilitación de información en razón de especiales circunstancias. Podrá exigirse por la información una retribución, la cual no Podrá exceder de los gastos directamente imputables a la facilitación de la información. No Podrá exigirse retribución en los casos en que por circunstancias especiales existiere motivo fundado para creer que se ha llevado a cabo un almacenamiento inexacto o ilícito de datos personales, o en los casos en que la información facilitada hubiera revelado que los datos personales debieren ser rectificados o, en virtud de lo dispuesto en el articulo 27, tercer párrafo, proposición segunda, semiproposición primera, hubieren de ser cancelados. Los párrafos primero y segundo no regirán en la medida en que: 1. el dar a conocer datos referidos a personas pudiera crear un peligro considerable para el objeto social o los fines del ente almacenante, y no obstaren a ello intereses legítimos del afectado, 2. el servicio publico competente con relación al ente almacenante hubiere observado que el dar a conocer datos referidos a personas podría poner en peligro la seguridad o el orden públicos o causar otros perjuicios para el bien de la Federación o de un Estado, 3. los datos

personales hubieren de ser mantenidos en secreto en virtud de una norma jurídica o por razón de su esencia, en especial a causa de intereses legítimos preponderantes de una tercera persona, 4. los datos personales hubieren sido tomados de fuentes de acceso general, 5. los datos personales que, en virtud de lo dispuesto en el articulo 27, segundo párrafo, proposición segunda, estuvieren bloqueados porque sobre la base de disposiciones legales, estatutarias o contractuales, no pudieren ser cancelados a tenor de lo dispuesto en el articulo 27, tercer párrafo, proposición primera (art. 26 LFAPD).

obtenidos directamente mediante un proceso de datos, tanto si fueren datos difundidos por el ente almacenante, como si son datos conservados por la entidad para su examen, en especial para su búsqueda automática (art. 4-2). En este sentido, la *comunicación* de datos personales, con el lleno de los requisitos previstos en la ley, bien puede hacerse a personas como entidades públicas tanto en los procesos de datos de carácter público (art. 11), como en los procesos de índole privada (art. 32).

Cancelar es la acción de hacer irreconocibles datos ya almacenados: cualquiera que fuere el procedimiento empleado a tal efecto. En tanto *modificar*, se considera la acción de transformación del contenido de datos ya almacenados (art. 4-3 y 4-4). En el caso de los datos de carácter privado, la *modificación de los datos* personales será admisible dentro del marco de los fines de una relación contractual o de una relación de confianza análoga a la relación contractual creada, respectivamente con el titular de los datos, o en la medida en que fuere necesaria para salvaguardar intereses legítimos de la entidad almacenante, y no existiere motivo fundado para creer que de ello pudieren resultar perjuicios para los intereses dignos de protección del interesado (art. 25).

La *Rectificación, bloqueo y cancelación de datos*, son tres acciones íntimamente ligadas y subsecuentes por la consideración de sí los datos almacenados, son : a) inexactos o se duda sobre su exactitud. El *in dubio pro date*, como podríamos llamarlo siempre favorece al titular de los datos. b) Si han sido almacenados de forma ilícita, c) Si los datos dejado de ser necesarios para los fines para los cuales fueron almacenados; y, d) porque así Alo exige@ el titular de los datos (Aafectado@).

Sin embargo, la rectificación de los datos sólo es procedente en el caso de no ser exactos los datos personales (art. 14 y 27 *ab initio*).

Se procederá al bloqueo de datos, cuando su exactitud fuere discutida por el titular de los mismos y no fuere posible determinar su exactitud ni su inexactitud. Igualmente serán bloqueados los datos cuando su conocimiento hubiere dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas a éste encomendadas, a menos que fueren imprescindibles para fines científicos, para fines probatorios, Aintereses preponderantes del servicio almacenante o de un tercero@, o por consentimiento del titular de los datos. Esto rige para los datos con carácter público como los de carácter privado.

La cancelación de datos, en los datos de carácter público, procederá cuando su conocimiento hubiere dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas comprendidas dentro de su competencia y no existieren motivos fundados para creer que la cancelación pudiera causar perjuicio a intereses dignos de protección del titular. Igualmente serán cancelados los datos si su almacenamiento hubiere sido ilícito o cuando así lo exigiere el interesado. En los datos de carácter privado, además de los anteriores casos, procederá la cancelación cuando así lo exigiere el interesado, en los datos referentes a condiciones de salud, acciones punibles, infracciones de policía, así como a concepciones religiosas o políticas, si su exactitud no pudiere ser probada por la entidad almacenante (art.14 y 27 *in fine*).

El *habeas data* y el grupo de derechos subsecuentes rigen para los titulares de datos cuando sean almacenados tanto en un Aproceso de datos de autoridades y otros servicios públicos@ (art.7 y ss LFAPD), o procesos informatizados de carácter público, como en los A procesos de datos de entes no públicos para uso interno A (art. 22) y los Aprocesos de datos realizados con finalidad mercantil para entes no públicos@, vale decir de carácter privado o que se reputan privados a los efectos de

la LFAPD, respectivamente (v.gr. el caso de las Aempresas públicas de derecho público@, art.31).

4.2.1.3. DEFINICIONES APLICABLES AL PROCESO INFORMATIZADO DE DATOS.

La LFAPD, estructura tres procesos de datos, a saber: a) El Proceso de datos de autoridades y servicios públicos (arts. 7 a 21); b) El proceso de datos de Aentes@ no públicos para uso interno (arts. 22 a 30); y c) El proceso de datos realizado con finalidad mercantil para entes no públicos (arts. 31 a 40). En estos procesos de datos de naturaleza jurídica de derecho público y de derecho privado, respectivamente, rige por igual etapas o fases, principios, derechos y deberes de los titulares de los datos, a pesar de estar regulados por separado, pues la misma norma reiterada como innecesariamente los reglamenta para cada uno, con específicas diferencias v.gr. sobre el derecho de Afacilitación de información al afectado@ (arts. 14, 27 y 34), con cuasi similar contenido para cada uno de los procesos.

Interesa a los propósitos de la investigación, desentrañar las etapas ínsitas en dichos procesos, cara a la estructuración del procedimiento informatizado de datos informáticos, el cual abordaremos en la Parte III, *in fine*.

En efecto, las etapas o fases inmersas en el *proceso alemán de datos* inmersa en las tres clases de procesos de datos son: a) La etapa de recolección o de Aelaboración@ de datos; b) La etapa de almacenamiento; c) La etapa de conservación e inscripción en un registro (público, privado o mixto, según fuere el caso); y d) La transmisión o comunicación de datos; y e) Rectificación, bloqueo y cancelación de datos [145].

La LFAPD, al hablar del proceso de datos, en general, estipula que a éste debe someterse los titulares de los datos o interesados, si así esta previsto en una ley o norma jurídica en forma expresa o si el interesado así lo consiente en forma

escrita, Asiempre que no procediere otra forma en razón de especiales circunstancias@ (art. 3 LFAPD).

Igualmente, interesa aquí destacar los conceptos estructurales del derecho de habeas data y el de Aarchivo informatizado@ que están íntimamente ligados con el concepto de proceso de datos. En efeto, se considera *archivo informatizado*, una colección de datos estructurados de manera homogénea, susceptibles de ser obtenidos y ordenados de conformidad con determinadas características y, en su caso, reordenados y explotados de conformidad con otras características determinadas, cualquiera que fuere el procedimiento empleado a tal efecto, sin se consideren comprendidos los expedientes y las colecciones de expedientes, a menos que los mismos pudieren ser reordenados y explotados por procedimientos automáticos (art. 1-3).

---

(145) En la parte III, *in fine* de esta investigación proponemos una estructura de procedimiento informatizado de datos personales, basado en estas concepciones de la LFAPD y las emitidas por los doctrinantes Fermín Morales Prats y Vittorio Frosini.

Ahora, pasemos a ver otros aspectos capitales del procedimiento informatizado de datos alemán que aún hoy, tienen relevancia y discusión doctrinal no pacífica.

4.2.2. EL COMISARIO DE PROTECCIÓN DE LOS DATOS: UN OMBUSDMAN [146] EN EL SECTOR PUBLICO Y UN VEEDOR CIUDADANO EN EL SECTOR PRIVADO.

La figura del Comisario de datos personales en el proceso de datos alemán se estructura, cualifica y funciona, según la clase de proceso (público o privado) ante el cual se nombra o se designa por parte de las autoridades públicas federales o las personas privadas competentes, según fuere el caso y ámbito competencial.

4.2.2.1. EL COMISARIO FEDERAL DE PROTECCION DE DATOS EN EL SECTOR PUBLICO.

El nombramiento del Comisario Federal de protección de datos en Alos procesos de datos de autoridades y otros servicios públicos@, se realiza por el Presidente Federal a propuesta del Gobierno Federal. El nombramiento se extingue por expiración del plazo de mandato y por destitución, previo trámite legal y la entrega de un Ainstrumento fehaciente@ extendido por el Presidente Federal.

El designado como Comisario prestará su juramento y cumplirá un plazo de cinco (5) años y su régimen jurídico será el de derecho público. Jerárquicamente depende el Ministerio Federal del Interior, quien podrá entre otras atribuciones, encomendar a un sustituto del Comisario, cuando el titular se viere impedido para ejercer el cargo.

El Comisario Federal de Protección de Datos, tiene las siguientes funciones:

a) *De cumplida ejecución y de asesoramiento sobre leyes de protección de datos*. En consecuencia, velará por la observancia y cumplimiento de la LFAPD;

---

(146) ORTI VALLEJO, A. Ob. ut supra cit., pág. 13

así como de otros preceptos sobre protección de datos a los cuales están obligados las autoridades públicas y otros servicios públicos de la Federación, para corporaciones, instituciones y fundaciones de derecho público, etc. Se exceptúa de esta previsión los Tribunales, en la medida en que estos no conocieren de negocios contencioso-administrativos. A este efecto podrá formular recomendaciones en orden al mejoramiento de la protección de datos, pudiendo en especial asesorar al Gobierno Federal y a los distintos Ministros, así como a las restantes autoridades públicas en todo lo tocante a la protección de datos.

b) *De Emisión de dictámenes e informes*. Si fuere requerido a ello por Ala Dieta Federal Alemana Ao por el Gobierno Federal, el Comisario Federal deberá emitir dictámenes e informes. Asimismo elevara anualmente a la Dieta Federal Alemana una memoria de su actividades.

c) *De solicitud de auxilio a autoridades y servicios públicos*. El Comisario podrá solicitar a las autoridades y servicios públicos le faciliten información en relación con las preguntas que éste formulare, así como facilitarán el examen de toda clase de documentos y expedientes que guardaren relación con la elaboración de datos referidos a personas, especialmente los datos almacenados y los programas de ordenador. Y, como consecuencia, permitirán en todo momento el acceso a todos los locales oficiales.

d) *De Registro*. EI Comisario Federal llevará un registro de los archivos explotados automáticamente, en los cuales se almacenaren datos referidos a personas. Dicho registro se limitará a contener un cuadro general de la naturaleza de los archivos y de los fines para los cuales fueren empleados. El registro podrá ser examinado por toda persona. Las autoridades, servicios y entidades públicas, estarán obligadas a denunciar al Comisario Federal los archivos explotados automáticamente por las mismas. Quedan exentos de esta obligación : La Oficina Federal de Defensa Constitucional, el Servicio Federal de Investigación y el Servicio de Contraespionaje Militar (art. 19).

e) *De reclamaciones*. Si el Comisario Federal de Protección de Datos observare que con ocasión del proceso de datos personales se atenta contra LFAPD, o contra las normas jurídicas de protección de datos, formulará una reclamación ante la autoridad suprema federal competente, si se tratare de la Administración Federal; ante la Dirección del Ferrocarril Federal, si se tratare de este; ante la Dirección o, en su caso, ante el órgano que tuviere atribuida la representación, si se tratare de corporaciones, instituciones o fundaciones de Derecho publico directamente dependientes de la Federación, así como si se tratare de agrupaciones de tales

corporaciones, instituciones y fundaciones; y la intimara a que se pronuncie dentro de un plazo que el mismo fijara (art. 20).

f) *De protección de los derechos de los titulares de datos personales*. Toda persona podrá acudir al Comisario Federal de Protección de Datos si fuere de la opinión de que en el curso del tratamiento de sus datos personales realizado por las autoridades, servicios y entidades públicas, a excepción de los Tribunales, siempre que estos no conocieren de negocios contencioso-administrativos, han lesionada los derechos de aquéllas (art. 21).

4.2.2.2. EL COMISARIO DE PROTECCIÓN DE DATOS EN EL SECTOR PRIVADO.

La LFAPD, si bien distingue los Aprocesos de datos de entes no públicas para uso interno@ y los Aprocesos de datos realizados con finalidad mercantil para entes no públicos@, no procede de idéntica manera, cuando menos, respecto de las funciones generales y especiales que el Comisario de Protección de los datos en el sector privado debe cumplir en uno y otro procesos.

En efecto, cuando se trata de procesos de datos de entes no públicos para uso interno, la designación del Comisario de Protección de datos se realizará, según el art. 28 de la LFAPD, por las personas, sociedades y otras agrupaciones de personas de derecho privado que sometan a tratamiento (o elaboraren) automáticamente datos personales y a tal efecto ocuparen con carácter permanente, por regla general, a cinco trabajadores por lo menos, deberán nombrar por escrito, lo mas tarde dentro de un mes después de iniciar su actividad, a un Comisario de Protección de Datos. Igual se procederá si se ocupare con carácter permanente a veinte trabajadores.

El Comisario de Protección de Datos dependerá directamente del propietario, de la Dirección, del gerente o de otra persona a quien correspondiere la dirección en virtud de disposición legal o estatutaria. En la aplicación de su pericia profesional en

materia de protección de datos no estar sujeto a instrucciones superiores. No podrá ser objeto de perjuicios por razón del cumplimiento de sus funciones.

El Comisario de Protección de Datos, cuando se trata de Aprocesos de datos realizados con finalidad mercantil para entes no públicos@, se designará por las personas, sociedades y otras agrupaciones de personas de derecho privado, o en su caso, por las empresas de derecho público que concurrieren en el mercado, según el art. 38 de la LFAPD. En cuanto a las funciones generales y especiales, éste Comisario cumplirá, en cuanto fuere procedente, las que se atribuyen al Comisario en el proceso de datos de entes no públicos para usos internos.

En tal virtud, El comisario de Protección de Datos, para uno y otro proceso de datos, cumple en su ámbito competencial idénticas funciones generales a las atribuida al Comisario Federal de Protección de Datos; vale decir, que velará por la observancia, cumplimiento y conocimiento de la LFAPD; así como de otras disposiciones relativas a la protección de datos. A tal efecto podrá acudir en casos de duda a la Autoridad de tutela (autoridades administrativas o jurisdiccionales, según el caso).

Como funciones especiales tendrá: a) *De veeduría y vigilancia de datos, fines, destinatarios y equipos.* En tal virtud, llevará un estado de la clase de los datos personales almacenados, así como del objeto social y los fines para cuya realización o cumplimiento fuere necesario conocer tales datos, de sus destinatarios regulares y la clase de los equipos de tratamiento automatizado de datos que estuvieren instalados;

b) *De veeduría de medios informáticos.* Velará por la regularidad de la aplicación de los programas de ordenador con cuya ayuda debieren ser tratados los datos personales; y,

c) *De veeduría profesional.* Prestan asesoramiento en la selección de las personas que se hubieren de ocupar en el tratamiento de datos los personales.

4.2.3. SISTEMA PUNITIVO Y SANCIONADOR EN MATERIA DE DATOS PREVISTO EN LA LFAPD.

Siendo la LFAPD, una ley de ámbito federal, su carácter es de ley general, por tanto, se aplicará subsidiariamente en caso de ausencia de ley especial o para llenar vacíos o lagunas legislativas si existieren otras leyes de protección de datos de ámbito federal (art. 45). En materia punitiva se aplicarán preferentemente a la LFAPD, a título de ejemplo las siguientes disposiciones: a) Sobre el derecho a negarse a extender certificaciones o a facilitar información por razones personales o profesionales en procedimientos judiciales (arts. 52 a 55 de la Ordenanza Procesal Penal); b) Sobre la obligación, limitación o prohibición del almacenamiento, difusión o publicación de indicaciones pormenorizadas sobre personas (art. 161 de la Ordenanza Procesal Penal); y, c) Secreto profesional (v.gr. secreto médico. Art. 203 Código Penal) [147].

Sin embargo, la LFAPD, se aplicará con carácter general en los casos expresamente previstos como hechos punibles (delitos y contravenciones) contra el tratamiento (informatizado o no) de datos personales.

1. Delitos (art. 41 LFAPD):

a) *Atentados contra los datos personales que no son de dominio público.*

Se considera como hecho punible, perseguible a instancia de parte el que sin la debida autorización: 1. comunicare o modificare, o 2. recuperare o se procurare a partir de archivos encerrados en depósitos adecuados, datos referidos a personas y protegidos por la LFAPD, que no fueren de dominio público, será castigado con pena de privación de libertad de un año como máximo o con pena de multa.

---

(147) Véase otros ejemplos en el apartado 4.2.1

b) *Tipo Agravado por el lucro o por perjuicio a otro.*

Si el autor, realizare una cualesquiera de la anteriores conductas y además obrare por precio o con el propósito de procurarse a si mismo o a otro un lucro o de causar perjuicio a otro, la pena será privativa de libertad de dos años como máximo o de multa.

2. Contravenciones o AInfracciones@ de policía (art. 42 Ibídem). Obra con dolo o culpa quien: a) *Por falta de información al interesado de almacenamiento de datos que le conciernen*. No informar al interesado (Aafectado@), sobre el almacenamiento de datos personales que le conciernen por primera vez , a menos que hubiere tenido conocimiento del almacenamiento por otros medios. Igual incumplimiento se dará, si por primera vez fueren comunicados datos acerca de la persona interesada, siendo que debía ser informada de su almacenamiento, a menos que hubiere tenido noticia de éste por otros medios.

b) *Por falta de designación, teniendo la obligación de hacerlo, de un Comisario de Protección de datos.* Por incumplimiento de designar un Comisario de Protección de datos, por parte de las personas, sociedades y agrupaciones de derecho privado que sometan a tratamiento informatizado datos personales y que ocuparen permanentemente trabajadores (cinco o veinte)

Igual, sucederá cuando se incumple la obligación de designar Comisario de Protección de datos por parte de las personas, sociedades y agrupaciones de derecho privado dentro de los procesos de datos realizado con finalidad mercantil para entes no públicos.

c) *Por falta de adjunción de motivos que justifiquen un interés legítimo para la comunicación de datos*. Si el destinatario no justificare los motivos y la existencia de un interés legítimo y los medios que lo acreditaren en forma fidedigna y detallada para que sea admisible la comunicación de datos personales

d) *Por falta de cumplimiento del Adeber de denuncia@.* Cuando las personas, sociedades y otras agrupaciones de personas de derecho privado, así como sus filiales y sucursales, teniendo la obligación de formular en tiempo oportuno (un mes) denuncia, no lo hacen. Igual incumplimiento se verificará, si estas personas no facilitaren al formular tal declaración los datos necesarios o no los facilitaren correctamente o de manera incompleta. Estos datos se refieren a la determinación del propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y sobre personas encargadas de la dirección del tratamiento de datos y sus direcciones (art.39-2 y 3 LFAPD) **[148]**

e) *Por incumplimiento en la facilitación de información pertinente o no tolerase el acceso a terrenos y locales para ante la Autoridad de Tutela.* Las personas, sociedades y otras agrupaciones de derecho privado, que teniendo la obligación de facilitar sin demora, si fueren requeridas para ello, las informaciones necesarias para el complimiento de las funciones de la Autoridad de Tutela, no facilitare una información o no la facilitare correcta o completamente, o no la facilitare en tiempo oportuno, o, incumpliendo las funciones de vigilancia encomendadas por la Autoridad de Tutela para penetrar en los inmuebles y locales de negocio del ente, y llevar a cabo en ellos inspecciones y comprobaciones y para examinar documentos de la explotación, en especial el estado que debiere ser llevado por el Comisario de Protección de Datos, y examinar los datos almacenados y los programas de tratamiento

La conducta antirreglamentaria podrá ser sancionada con pena de multa de cincuenta mil marcos alemanes como máximo.

---

(148) *LFAPD. ART. 39. Deber de denuncia*. Las personas, sociedades y otras agrupaciones de personas que se mencionan en el articulo 31, así como sus filiales y sucursales, deberán dar cuenta de la iniciación de su

actividad ante la autoridad de tutela competente dentro del plazo de un mes. Al Llevar a cabo la denuncia, deberán comunicarse al Registro llevado por la Autoridad de tutela los siguientes datos: 1. nombre o denominación del ente; 2. propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y personas encargadas de la dirección del tratamiento de datos; 3. dirección; 4. objeto social o fines del ente y del tratamiento de datos; 5. naturaleza de los equipos utilizados para el tratamiento automatizado de datos; 6. nombre del Comisario de Protección de Datos; 7. naturaleza de los datos personales almacenados por el ente o por encargo suyo; 8. en caso de comunicación regular de datos personales, destinatarios y naturaleza de los datos comunicados. El primer párrafo regirá en cuanto fuere procedente para la terminación de la actividad, así como para la modificación de los datos facilitados en virtud de lo dispuesto en el segundo párrafo.

4.3. LA EUROPA DE 1980: EL COMIENZO DE UNA DÉCADA CLAVE EN LA NORMATIZACIÓN Y NORMALIZACIÓN DEL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES.

Si bien es cierto Alemania, Suecia, Francia; entre otros Estados europeos, habían afrontado no solo teórica sino prácticamente el complejo mundo del tratamiento informatizado de datos de carácter personal, como el movimiento, flujo o circulación de datos entre países, expidiendo leyes sobre la materia; no es menos cierto también, que éstos esfuerzos legislativos resultaban aislados e incomprensibles incluso en el contexto de una Europa unida, pregonada y defendida desde hacía tres décadas antes con la suscripción de Francia y Alemania con la llamada Adeclaración o Plan Shuman@ de 1950, y subsiguientemente la suscripción del ATratado del Carbón y el Acero@ de 1951--CECA--, por los países bajos, Italia, Bélgica, Luxemburgo y la entonces República Federal Alemana (RFA). Mucho más, resultaba incomprensible cuando dichos Estados habían apostado por una Comunidad de Estados europeos, de origen económico sí, pero luego su radio ampliado a los aspectos sociales, laborales, culturales, políticos, legislativos; y en fin, en un futuro no muy lejano, alcanzar lo siempre buscado: un gran Estado Europeo unido con una sola Constitución, como lo teoriza el profesor alemán de la Universidad de Münster, *Martín Seidel* **[149]**

Pese a ello, el profesor *Davara* **[150]**, sostiene que desde 1967 en Europa existía Aconciencia europea sobre protección de la privacidad@ (por la traducción

literal de la Aprivacy@ anglosajona) y para ello relaciona varias recomendaciones surgidas en el seno del Consejo de Europa, el cual constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona, entre los que estaba la Intimidad. Entre las más destacadas están: a) La Resolución 509 de 1958, de la Asamblea del Consejo de Europa, sobre ADerechos

---

(149) Vid., RIASCOS GOMEZ, Libardo O. *LOS DENOMINADOS RECURSOS ANTE LOS TRIBUNALES DE JUSTICIA DE LA C.E. Y ANDINO.* Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, pág. iii y 1 a 3.

(150) DAVARA RODRIGUEZ. Miguel A. *MANUAL DE DERECHO INFORMATICO.* Ed. Aranzadi S.A., Pamplona (Nav.), 1997, pág. 56-61.

Humanos y los nuevos logros científicos y técnicos@, b) Las recomendaciones del Comité de Ministros del Consejo de Europa de 1973 y 1974, sobre la creación de bancos de datos en el sector privado y público, respectivamente, c) En Septiembre de 1980, la Recomendación de la OCDE, sobre el flujo internacional de datos, protección a la intimidad y las libertades fundamentales, d) Recomendación del 30 de abril de 1980, relativa a la enseñanza, la investigación y la formación en materia de Ainformática y derecho@, e) La Recomendación del 18 de septiembre de 1980, relativa al intercambio de informaciones jurídicas en materia de protección de datos, f) La Recomendación del 23 de enero de 1981, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados, g) La Recomendación del 23 de Septiembre de 1983, relativa a la protección de los bancos de datos de carácter personal utilizados con fines de investigación científica y de estadísticas, h) La Recomendación de 23 de enero de 1986, relativa a la protección de los datos de carácter personal utilizados con fines de seguridad social@.

Con base en éstos o por inspiración de aquellos, algunos Estados Europeos expidieron sus propias normas de ámbito nacional, relativas al tratamiento informatizado de datos, con marcadas diferencias tanto en la conceptualización de los términos técnico-jurídicos (datos, fichero, banco de datos, tratamiento Aautomatizado@, etc), como en lo referente a la enunciación y enumeración de

principios, derechos, deberes y excepciones al tratamiento y la protección de los datos, lo cual indicaba que no existía univocidad en los temas referidos, en el grado y categorías de protección que estilaban dispensar a los datos de carácter personal sometidos a tratamiento informatizado en uno y otro país, ni menos el ámbito de los derechos fundamentales que en éste se involucraban si no era únicamente el de la intimidad.

Orti Vallejo [151] , estima que esta etapa de legislación estatal de protección de datos, se caracteriza por la preocupación de tutelar la intimidad de la persona, como lo acredita el hecho de que se protejan las informaciones consideradas sensibles, que son aquellas que tienen una más inmediata incidencia sobre la vida privada y sobre el

---

(151) ORTI VALLEJO. A. Ob. ut supra cit., pág. 15

ejercicio de las libertades. Cierto es que esta etapa, también se comienza a introducir una mayor libertad en la creación de ficheros de datos personales, pero, como contrapartida, se otorgan más garantías al derecho de las personas a conocer sus datos contenidos en ficheros o banco de datos mediante el derecho de acceso y consecuentemente a rectificar o cancelar informaciones inexactas o indebidamente procesadas. Sin embargo, como hemos visto y abundaremos sobre ello, esta época legislativa de protección de datos produjo dos enclaves actualmente vigentes: por un lado, el matrimonio de las leyes de protección de datos aparentemente únicamente con el derecho a la intimidad, produjo a partir de ésta época una identificación casi plena sustentada en la argumentación de que la informática atentaba directa y plenamente a la intimidad y no al conjunto de derechos y libertades fundamentales, tal como se revelaría en las diversas normas protectoras de datos personales; y por otro lado, considerar al derecho de *habeas data* como una sola emanación del derecho anglosajón del *habeas corpus* y de aplicación exclusiva al tratamiento de la información manual o mecanizada, sino también, a todo procedimiento de tratamiento de datos personales de carácter informatizada. Esto replanteaba el tradicional de Aderecho de acceso@ a la información que tiene toda persona sobre

los datos que le conciernen, así como los facultades subsecuentes, de conocimiento, consulta, rectificación, bloqueo y cancelación de información o datos personales que sean erróneos, inexactos o ilegales

De ésta época, tomaremos como prototipo de análisis y estudio las normas supraestatales o comunitarias de protección de datos personales que tendieron desde aquella época hasta los actuales momentos por la normatización y normalización del tratamiento informático de datos personales, la protección integral de los derechos, libertades públicas (o Aindividuales@) e intereses legítimos. En efecto, abordaremos la Recomendación del Consejo de la OCDE, del 23 de Septiembre de 1980, cuyo ámbito se extiende a los Estados de la Comunidad Europea (hoy, UE) y los algunos Estados de Oriente y Occidente. Así mismo. En efecto, el Convenio de Estrasburgo de 28 de Enero de 1981, el cual creo un espíritu normalizador de todo cuanto existía en Europa sobre tratamiento informatizado de datos personales.

4.3.1. LA RECOMENDACIÓN DEL CONSEJO DE LA OCDE, DE SEPTIEMBRE DE 1980

La OCDE (Organización de Cooperación y Desarrollo Económico), creada en 1948, como organización de cooperación preferentemente económica entre Estados Europeos que hoy forman la UE (Unión Europea), EE.UU y Canadá (1960), Japón (1964), Finlandia (1969), Australia (1971) y Nueva Zelandia (1973). Sin embargo, las funciones de esta organización internacional de Estados también se dirige desde su nacimiento hasta la actualidad a proyectar, planear, desarrollar, emitir conceptos, sugerencias y recomendaciones sobre diferentes aspectos de la vida que inciden de alguna manera en lo económico, tales como las estrategias, políticas y directrices sobre la protección de derechos fundamentales, libertades públicas e intereses legítimos de las personas naturales, jurídicas, públicas o privadas, según fuere el caso, con miras esencialmente ha facilitar la armonización de las legislaciones nacionales de los diferentes Estados que componen la OCDE.

En éste último orden de ideas, la OCDE recomendó a sus Estados Miembros, sin perjuicio de sus legislaciones internas sobre la materia [152], unas directrices sobre la protección de derechos fundamentales, como el de la intimidad, las Alibertades individuales@, y sobre todo el derecho a la información que tiene toda persona y Aconciliar valores fundamentales aunque susceptibles de entrar en conflicto, tales como la intimidad y el libre flujo de la información@ (Preámbulo del Convenio). Esta recomendación previos los proyectos y estudios, por parte de las comisiones y subcomi-

---

(152) El artículo 5 del Convenio de 14 de diciembre de 1969, de la OCDE, expresa: "Con miras a alcanzar sus objetivos, la Organización, podrá: a) adoptar decisiones que, salvo disposición en contrario, vincularan a todos los miembros: b) formular recomendaciones a los miembros; c) concertar acuerdos con sus miembros, con Estados no miembros y con organizaciones internacionales". Por su parte, el articulo 18 del Reglamento de Procedimiento de la OCDE, de julio de 1976, dispone: "a) Las decisiones de la Organización, adoptadas de conformidad en los artículos 5, 6 y 7 del Convenio, podrán ser: (i) decisiones obligatorias para sus miembros, y que estos ejecutarán previo cumplimiento de los procedimientos que requieren sus constituciones; (ii) decisiones por las que fueren aprobados acuerdos concertados con sus miembros, con Estados no miembros y con organizaciones internacionales; (iii) decisiones de orden interno relativas al funcionamiento de la Organización, que se denominaran resoluciones; (iv) decisiones por las que se hicieren comunicaciones a Estados no miembros o a organizaciones. b) *Las Recomendaciones* de la Organización, formuladas de conformidad con lo dispuesto en los artículos 5, 6 y 7 del Convenio, serán sometidas a la consideración de los miembros para que estos procedan a su ejecución si lo estimaren oportuno, c) los textos de las Decisiones o de las Recomendaciones a que se alude en los apartados a), (i) y b) que anteceden, deberán incluir una referencia al articulo 4- a) o al articulo 5-b), respectivamente". Citado por RIVERA LLANO, A. Ob.cit.,p.178.

siones de expertos respectivas se concretó en lo que se conoce como ARecomendación Adoptada por el Consejo de la OCDE (con base en los arts. 1 (c), 3 (a) y 5 (b) del Convenio relativo a la OCDE, de 14 de diciembre de 1960) del 23 de Septiembre de 1980, *Apor la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales@.*

El Texto de la Recomendación propuesto al Consejo por el Comité de Política Científica y Tecnológica, fue aceptado por los Estados Miembros de la

OCDE, entre los que Estaba España, Alemania Occidental, Austria, Bélgica, Dinamarca, EE.UU., Finlandia, Francia, Grecia, Italia, Japón, Luxemburgo, Noruega, Nueva Zelandia, los Países Bajos, Portugal, Suecia y Suiza; en tanto que, Islandia, Turquía y el Reino Unido adhirieron a la Recomendación, el 21 de enero de 1981 y el 27 de Octubre de 1981, respectivamente, no sin mantener su abstención por lo que se había sostenido en la sesión de 23 de Septiembre de 1980.

La Recomendación de la OCDE, constituye un documento de capital importancia para aquella época e incluso con plenas y claras incidencias en la actualidad, tanto en las legislaciones internacionales como en las comunitarias europeas [153]. El documento preparado por un grupo heterogéneo de expertos de diferentes Estados de Occidente y Oriente del mundo, es un fiel, serio, oportuno y claro diagnóstico y recetario de los innumerables hechos, sucesos, problemas, conflictos y proposición de sugerencias y soluciones a los mismos, sobre todo lo atinente al *flujo internacional de datos* entre países miembros de la OCDE y la protección de los derechos fundamentales como el de la intimidad (aunque no en todo su contexto, pues sólo se destaca la visión iusinformática de la intimidad), como hace énfasis el preámbulo, el texto y contexto y las Memorias Explicativas (en adelante M.E.) de la Recomendación; además del conjunto de las llamadas *libertades individuales* (surgidas en la historia del constitucionalismo del liberalismo anglo-francés, y que hoy se consideran como un ám-

---

(153) El profesor destaca esa importancia de la Recomendación de la OCDE, pero más dirigida a la vocación legislativa de los Estados Miembros que con vocación europeísta, y más aún, internacionalista, tal y como fue su origen y presentación. DAVARA RODRIGUEZ, Miguel. *MANUAL DE DERECHO INFORMATICO*... Ob.cit., pág. 57.

bito importante de los derechos fundamentales) [154], dentro de las cuales se encuentra el hoy llamado Aderecho de habeas data@, el derecho a la información y los derecho de impugnación y recurso que tiene toda persona contra decisiones administrativas o judiciales.

La Recomendación de la OCDE, en el anexo correspondiente a las A *directrices sobre protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras@,* estructura las cinco partes en las que se compone. Estas están referidas a las generalidades, Los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales aplicables en el ámbito internacional: libre circulación y restricciones legítimas, la aplicación de los principios en el ámbito interno; y, la cooperación internacional.

A nuestros efectos destacaremos, los siguientes temas: a) las definiciones en el tratamiento informatizado de los datos personales y, b) los principios y excepciones fundamentales del tratamiento informatizado de los datos, tanto en el ámbito nacional como en el ámbito internacional, y dentro de éste especialmente, el principio denominado de la *libre circulación de datos personales* y las restricciones legítimas.

---

(154) La importancia mundial que han adquirido los derechos fundamentales en el ámbito del derecho constitu- cional español a tenido relevancia muchísimo antes del reconocimiento constitucional en 1978, tal y como lo sostiene *SEMPERE,* al referirse a la ATutela constitucional de los derechos fundamentales de la per- sonalidad@, y en especial *al derecho a la intimidad* prevista en el art. 18 CE, que en el momento de la entrada en vigor del texto constitucional ya existía un cuerpo consolidado de doctrina y jurisprudencia con el reconocimiento y tutela de los derechos del honor, la intimidad, la imagen; entre otros. En igual forma, se suma a ello, que con carácter preconstitucional la protección de los derechos fundamentales, tanto en el ámbito penal (doctrina del T.C., sobre los delitos de injurias y animus iniuriandi y una nueva regulación del C.P.) como en el ámbito de la tutela civil (L.O.1/1982, de 5 de Mayo), así como en relación con la compatibilidad de uno u otro tipo de tutela y la posibilidad de elección, entre ellos, por el interesado. Tal reconocimiento determina, al menos, cuatro consecuencias a destacar: 1. El reconocimiento de los derechos privados de la personalidad mencionados en el artículo 18 como derechos fundamentales. El mismo conlleva una doble consecuencia. Por un lado, afirmar que ya no tiene mucho sentido hablar de estos derec*hos como derechos subj*etivos de naturaleza privada, sino como derechos fundamentales de la personalidad, tal como lo sostiene *DIEZ PICAZO*. Por otro lado, en el ejercicio y limitaciones de estos derechos debe aplicarse la doctrina del T.C., sobre los derechos fundamentales. 2. Exigencia de garantía frente al legislador ordinario. Se concretaría en el respeto por parte de las leyes que reg*ulen el ejercicio* de estos derechos, de un contenido mínimo esencial (art. 53.1 CE). Concepto éste jurídicamente indeterminado cuyo control corresponde, en últ*imo término, al TC (a*rt.12), a través del recurso de inconstitucionalidad, recurso con el que se garantiza la primacía de la C.E. --arts. 161.1. a) CE y 27 y 55.2 de la L.O.T.C. 3. *Cualificación de la interven*ción del legislador: reserva de la ley orgánica. Implica que la ley que desarrolle el ejercicio de estos derechos, tanto en su aprobación como modificación, se ajuste a un procedimiento y quórum especiales (art. 168 CE), dado que se trata de leyes orgánicas (art. 81 y 82 CE). 4 . Habilitación de tutela especial ante el Tribunal Constitucional: Recurso de amparo.... SEMPERE RODRIGUEZ, Cés*ar. ARTICULO 18: DERECHO AL HONOR,* A LA INTIMIDAD Y A LA IMAGEN. En: COMENTARIOS A LA CONSTITUCION. Ob.ut supra cit.págs..390 y ss.

4.3.1.1. DEFINICIONES BASICAS EN EL TRATAMIENTO INFORMATIZADO DE LOS DATOS PERSONALES

Siguiendo el criterio --generalizado en la década de los ochenta-- la Recomendación de la OCDE, prevé una serie de definiciones iusinformáticas, tales como, Responsable del fichero, datos de carácter personal y flujos internacionales de datos de carácter personal. Se abstiene de definir lo que debe entenderse como Atratamiento automático de datos@, pese a que en el preámbulo y en el apartado tercero referido a los Agrados de sensibilidad de los datos@, se menciona expresamente. Las razones, entre muchas otras, son: limitar al máximo las definiciones; y en el caso específico, porque resulta difícil hacer una distinción clara entre tratamiento Aautomático y no automático de la información@ [155] y porque las directrices no están dirigidas exclusivamente al tratamiento de datos de carácter personal con Aordenadores@ (o Aautomático@), aunque curiosamente esto fue la punta del iceberg que convocó la reunión, estudio y planteamiento de las recomendaciones ahora comentadas [156].

La persona física a la que se refiere la definición tiene que gozar de una habilitación legal para decidir, sobre el contenido y utilización de los datos, independientemente de si los datos han sido o no obtenidos, registrados, tratados o difundidos por dicha persona o por una persona que obra en su nombre. El responsable del fichero puede ser una persona física o jurídica, una autoridad u organismo público.

---

(155) Cfr. MEMORIA EXPLICATIVA (M.E) Punto 34. A*Tratamiento automático y no automático de datos@.* Las actividades que la OCDE había venido dedicando a la protección de la intimidad y a otros ámbitos co- nexos estaban centradas en el tratamiento automático de la información y en las redes de ordenadores. El grupo de expertos considero con especial atención la cuestión de si el alcance de estas directrices debía o no quedar limitado al tratamiento automático e informatizado de los datos de carácter personal. Este enfoque puede justificarse por razones diversas, tales como los especiales peligros que llevan consigo para las libertades individuales la automatización y los banco de datos informatizados, el creciente predominio de los métodos de tratamiento automático de la información, en especial en el contexto de los flujos internacionales de datos, así como el marco especifico de la política de la información, de la informática y las comunicaciones, dentro del cual hubo de cumplir su mandato el grupo de expertos. AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla.Tratados Internacionales núm. 2.

(156) M.E. Punto 35. AAsí, por ejemplo, existen sistemas mixtos de tratamiento de la información y hay también ciertas etapas del tratamiento de la información que pueden o no ser susceptibles de automatización. Estas dificultades pueden agravarse aun mas como consecuencia de los continuos progresos técnicos, tales como la aparición de métodos semiautomáticos perfeccionados basados en la utilización de microfilmes o de microordenadores, que podrán ser empleados cada vez más para fines meramente privados, a la vez inofensivos e incontrolables. A mayor abundamiento, si las directrices se centraran únicamente en los ordenadores podrían dar lugar a incoherencias y lagunas, del mismo modo que podrían crear para los

responsables de ficheros posibilidades de obviar las normas de aplicación de la directrices con sólo utilizar medios no automáticos para fines que podrían ser nocivos@. Ibídem Ob. ut supra cit.

La definición excluye, por tanto a: a) las autoridades competentes para conocer autorizaciones o licencias y los organismos que autorizan el tratamiento de la información pero son competentes para decidir sobre que actividades deben llevarse a cabo y para que fines; b) las empresas de servicios informáticos que realizan actividades

de tratamiento de la información por cuenta de terceros; c) las autoridades competentes en materia de telecomunicaciones y los organismos análogos; d) los *usuarios dependientes*, que si bien pueden acceder a los datos, no están sin embargo autorizados para decidir sobre que datos deberían ser registrados o cuales utilizados (M.E. núm.40).

Los *Datos de carácter personal*, o simplemente datos personales, se considera cualquier información relativa a una persona física identificada o identificable --o también interesado-- (R.1-b). Las directivas se aplicarán tanto a los datos personales en el sector público como en el sector privado, siempre que acarrearen un peligro para la intimidad y las libertades individuales, a causa de la manera en que fueren elaborados o por razón de su naturaleza o del contexto en que fueren usados (R.2). En esta aplicación deberá observarse: a) las medidas de protección a las diversas clases de datos tanto en la obtención, almacenamiento, elaboración o difusión. b) que no se excluyen ni siquiera datos de carácter personal que de manera manifiesta no ofrecieren riesgo alguno para la intimidad y las libertades individuales [157], y c) que no se limitará la aplicación de las directrices a la Aelaboración automática@ de datos personales (R.3).

Los *flujos internacionales de datos de carácter personal,* se consideran a los movimientos de datos de carácter personal a través de las fronteras nacionales (R.1-c).

Aunque hace referencia a los flujos internacionales, las directrices no tienen en cuenta problemas hacia el interior de los Estados Federales. Los movimientos de

datos tendrán lugar a menudo mediante la transmisión electrónica, pero también pueden servirse de

---

(157) M.E. Punto 1 a 3. Los problemas prioritario que detectaron las comisiones y subcomisiones de expertos se refieren principalmente al derecho a la intimidad; la informática, la tecnología (de ordenadores, redes de comunicación), las telecomunicaciones, el derecho a la información y el de Ahabeas data@, aunque en el texto de la Recomendación y las M.E., se hace mención genérica al derecho de acceso a la información, a conocer, actualizar, cancelar o modificar los datos de carácter personal por el titular o interesado; el Atratamiento automático de la información. En particular se refieren a la intimidad en un concepto más amplio que el tradicional derecho de Asólo dejar a solas@ -- el AThe Right to Privacy@ anglosajón--, y algo que se convertirá en la cantinela de proposición de toda la Recomendación, al decir: Acon la expresión intimidad y libertades individuales constituye el aspecto más controvertido@ de todos cuantos se tratan en la Recomendación de la OCDE de 1980.

otros medios de transmisión, así como por vía satélite (M.E.núm. 42).

4.3.1.2. PRINCIPIOS Y EXCEPCIONES FUNDAMENTALES DEL TRATAMIENTO INFORMATIZADO O NO DE LOS DATOS PERSONALES.

Las partes segunda, tercera y cuarta de la Recomendación de la OCDE, se destinan a hacer referencia a los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales a aplicar en el ámbito internacional: libre circulación de los datos y restricciones legítimas y aplicación de los principios en el ámbito interno, que no es más que un aparte reiterativo de las gestiones administrativas, jurídicas, legislativas Ay de otra índole@ que los Estados Miembros de la OCDE deben adelantar para implementar los medios y mecanismos idóneos para aplicar los principios en sus ámbitos legislativos internos y hacer efectivas las medidas de protección del derecho a la intimidad y las libertades individuales **[158]**.

Los principios fundamentales aplicables al tratamiento informatizado o no de los datos personales en el ámbito nacional, según la directiva son: a) limitación de la colecta de los datos, b) calidad de los datos, c) especificación del fin, d) restricción del uso, e) garantía de la seguridad, f) transparencia, g) participación del individuo y h) responsabilidad.

En el plano internacional, los principios básicos aplicables al tratamiento (infor- matizado o no) de los datos personales, constituyen un complejo grupo de principios y límites que estructuran a su vez, el principio fundamental denominado: *libre circulación de datos personales* dentro de un flujo o movimiento internacional de los mismos.

---

(158) P.IV: *AAPLICACION DE LOS PRINCIPIOS EN EL AMBITO INTERNO*. 19. Los países miembros al aplicar en su ámbito interno los principios (parte II y III) deberán crear mecanismos jurídicos, administrativos y de otra índole, o instituciones, tendentes a proteger la intimidad y las libertades individuales con respecto a los datos de carácter personal. En especial, los países miembros deberán: a) promulgar una legislación interna idónea, b) fomentar y apoyar las reglamentaciones autónomas, bien en forma de códigos de deontología, bien en otra forma, c) poner a disposición de las personas físicas medios idóneos para ejercer sus derechos, d) instaurar sanciones y recursos para los supuestos de inobservancia de medidas de aplicación de los principios que se detallan en las partes II y III. e) velar porque no exista discriminación desleal alguna contra los interesados@.

4.3.1.2.1. PRINCIPIOS DEL TRATAMIENTO DE DATOS EN EL AMBITO NACIONAL.

Aunque se hace una distinción de los principios tanto en el ámbito nacional y el ámbito internacional, y dentro del primero en cada una de las fases del tratamiento de los datos personales (recolección, almacenamiento, registro, difusión y flujo), lo cierto es que dichos Aprincipios son interdependientes y en parte se entrecruzan y traslapan. Por ello, las distinciones que con relación a los principios se hacen entre las actividades y las fases del tratamiento de datos son artificiales y no deben impedir que los principios sean tratados conjuntamente y estudiados como un todo@ (M.E.50). Esto se evidenció además, al analizar que los diferentes Estados Miembros de la OCDE, en sus diferentes iniciativas legislativas internas para la protección de la intimidad y las libertades individuales tienen muchos rasgos comunes, así como intereses, valores básicos y principios fundamentales [**159**] que guían y orientan las fases o ciclos del tratamiento de los datos personales.

Analicemos brevemente los mencionados principios:

1. El *Principio de limitación de la colecta de datos*, hace referencia a aquellos datos personales que, debiendo ser obtenidos por medios legítimos y leales,

y en el caso en que fuere procedente, con el conocimiento o el consentimiento del interesado, dichas
actividades deberán ser limitadas (R.7).

Este principio hace referencia a dos aspectos: a) los limites que han de fijarse a la colecta de aquellos datos que debieren ser considerados como especialmente datos

---

(159) Esos rasgos comunes se sintetizan así: a) Aponer límites a la colecta de datos personales, de conformidad con los objetivos del que hace acopio de tales datos y con otros criterios@, b) Arestringir el uso de los datos, de tal forma que se acomode a unos fines claramente expuestos; c) adoptar los medios necesarios para que el individuo conozca la existencia y el contenido de los datos y pueda requerir la corrección de los datos, y d) determinar las personas responsables del cumplimiento de las disposiciones y resoluciones de protección de la intimidad y de las libertades individuales que fueren aplicables. AEn términos generales, las leyes de protección de la intimidad y de las libertades individuales con relación a los datos de carácter personal tienden a cubrir las sucesivas etapas del ciclo que comienza con la colecta inicial de los datos y termina con la cancelación u otras medidas semejantes, y a garantizar en lo posible el conocimiento, participación y control del individuo con respecto a dicho ciclo@. M.E. núm. 5.

sensibles **[16 0]** a causa de la manera en que hubieren de ser tratados, su naturaleza, el contexto en el cual hubieren de ser utilizados, y b) las condiciones que deben cumplir los métodos de colecta de datos.

En cuanto al primer aspecto, hay que resaltar lo siguiente: Se deberá poner fin a la colecta indiscriminada de datos personales, y más aún cuando se trata de universalizar la consideración de qué datos se consideran sensibles. Para esto, la Recomendación suministra una serie de pautas que sirvan para determinar la índole de tales límites. Estas son: a) los aspectos cualitativos de los datos (es decir, que deberá ser posible extraer de los datos obtenidos una información de una calidad suficientemente buena, y que los datos deberán ser obtenidos dentro de un marco informativo apropiado); b) la finalidad del tratamiento de la información (es decir, que sólo deberán ser obtenidos determinados datos y, a ser posible la colecta de datos se limitará al mínimo necesario para lograr la finalidad prevista): (i) Identificación mediante "marcas" de aquellos datos que según las tradiciones y actitudes propias de cada país miembro fueren especialmente sensibles; (ii)

actividades de colecta de datos de determinados responsables de datos; (iii) preocupaciones relativas a los derechos humanos (M.E. núm. 51).

En cuanto al segundo aspecto, es decir las condiciones de los métodos de colecta

de datos, se advierte contra ciertas prácticas que implican, por ejemplo, el uso de dispositivos ocultos de registro de datos, tales como magnetófonos u otros que inducen a error a los interesados, moviendoles a facilitar información. La necesidad de poner los datos en conocimiento del interesado (que puede estar representado por un tercero, como

---

(160) Dado que por aquel entonces y hasta ahora, determinar el Agrado de sensibilidad de los datos@ resulta un labor titánica, aún cuando se acude a circunstancias específicas de potencialidad del riesgo, se consideró por los expertos de la Recomendación de la OCDE, hacer mención genérica de los Adatos sensibles@ para que sean los Estados Miembros quienes determinen cuáles se pueden considerar como tales. Se hacía mención por ejemplo, que mientras en unos países los Aidentificadores personales universales@ (tarjeta de identidad o cédula de ciudadanía, número de identificación profesional, de seguros, etc.), se consideran inocuos y útiles; en otros, se consideran algo delicado. Así mismo, se puso en evidencia, la disparidad de las legislaciones sobre qué datos se consideran o no sensibles. En efecto, en Alas legislaciones europeas existen precedentes al respecto --es decir, considerar datos sensibles a los datos referidos a la-- (raza, creencias, religiosas, registros de condenas, p.e.). Pero también se puede argüir que ningún dato es intrínsecamente privado o sensible, sino que puede llegar a serlo según su contexto y el uso que del mismo se haga. Esta opinión se refleja en la legislación de los Estados Unidos de protección de la intimidad, por ejemplo.(M. E. 50). En las partes III y IV., de esta investigación volveremos sobre el tema.

en el caso de los menores de edad o personas Adeficientes mentales@, etc.) o de obtener su consentimiento para registrarlos, constituye una norma básica, y el conocimiento, la exigencia mínima. Sin embargo, por razones prácticas, no es posible siempre exigir el consentimiento. p.e. las investigaciones criminales y la actualización periódica de las listas de distribución de correspondencia (M.E. núm. 52).

2. El *Principio de calidad de los datos*. Los datos personales deben ser pertinentes con respecto a los fines para los que fueron usados, y, en la medida en que fueren necesarios para tales fines, deberán ser exactos y completos, debiendo asimismo ser actualizados constantemente (R.8) .

La calidad de los datos hace relación a dos aspectos claramente definidos para toda información, más cuando ésta es de carácter personal. En efecto; uno, es el cumplimiento en todo el tratamiento (informatizado o no) de datos desde la recolección misma hasta la fase de difusión, recuperación o transmisión acerca de la finalidad con que han sido tratados los datos y su correspondiente utilización posterior; y otro, como verificación de lo anterior, el de que los datos tratados deberán ser exactos, completos y constantemente actualizados. Estos aspectos están interrelacionados, puesto que no se puede exceder en la utilización de los datos la finalidad para las cuales fueron tratados (informatizada o no) en su momento. v.gr. En los datos relativos a opiniones pueden fácilmente inducir a error si se utilizan para fines con los cuales no guardan relación alguna. Lo mismo puede decirse con respecto a los datos valorativos.

Sin embargo, se evidencia que en alguna clase de datos personales el criterio de la finalidad, lleva consigo el problema de si se puede o no causarse perjuicio a los interesados por falta de exactitud, de completud y de actualidad. Tal sería, el caso de las investigaciones de las ciencias sociales que llevan aparejados los llamados estudios "longitudinales" de la evolución de la sociedad, de investigaciones históricas y de actividades de archivo (M.E.núm. 53).

3. El *Principio de especificación del fin.* Los fines para los cuales se obtuvieren datos personales deberán ser precisados en el momento de la colecta de datos, debiendo su subsiguientemente uso limitarse al cumplimiento de tales fines o de aquellos otros que, sin ser incompatibles con los mismos, fueren especificados cada vez que fueren modificados (R.9).

Este principio reitera, complementa y concreta el anterior principio, poniendo énfasis en la relación utilización y finalidades previstas para el tratamiento (informatizado o no) de datos, los cuales deben precisarse desde el momento mismo de la recolección.

Los fines pueden ser definidos de maneras diversas y complementarias, principalmente por medio de declaraciones públicas, o bien informando a los interesados, por medio de la legislación, resoluciones administrativas y autorizaciones otorgadas por los organismos de tutela.

Así, cuando los datos hubieren dejado de estar subordinados a un fin y, siempre que fuere posible, podrá ser necesario hacerlos destruir (borrar) o darles forma anónima. Esto por cuanto, los datos dejan de tener interés, sucede que se pierde el control sobre ellos y pueden surgir nuevos riesgos, tales como, Ael hurto, reproducción no autorizada o de otras acciones ilícitas@ (M.E.núm. 54 *in fine*) .

4. El *Principio de restricción del uso*. Los datos personales deberán ser revelados, facilitados o, en general, usados para fines que no fueren los que se especificaren de conformidad con el anterior principio, excepto en los siguientes supuestos: a) previo el consentimiento del interesado, b) previa habilitación legal al efecto (R.10).

Este principio que limita el uso de los datos en ciertos y precisos casos, no es más que un principio bisagra de los principios relativos a la calidad y la determinación del fin, y como tal, juega un papel de inmovilizador de las facultades discrecionales que tuvieran las autoridades competentes, responsables de un fichero o incluso usuarios de los datos personales tanto en la revelación o divulgación como en el mera uso de los mismos. Por ello, se limita la divulgación o el uso de los datos que impliquen desviaciones con respecto a las finalidades previamente determinadas

La regla general, por la cual todo tratamiento de datos debe tener previamente determinadas sus finalidades desde el momento mismo de la recolección, precisa dos excepciones, a saber: una, por el consentimiento del interesado (o de su representante, en el caso de menores, etc.); y otra, por disposición normativa. Estas excepciones son *numerus clausus*, y por tanto, no cabe excepciones interpretativas según este principio.

En tal virtud, podría destinarse datos personales a fines de investigación, estadísticos y de planificación social, que inicialmente se han obtenido con miras a tomar decisiones de tipo administrativo, sin que media para ello, el consentimiento o así lo determine una norma jurídica.

5. El *Principio de garantía de la seguridad*. Deberán preverse medidas adecuadas de seguridad para proteger datos personales contra riesgos tales como la pérdida o el acceso, destrucción, uso, modificación o divulgación de los mismos sin la oportuna autorización (R.11).

Este principio constituye el epicentro de las medidas de protección del derecho a la intimidad y de las libertades individuales, cuando se ha sometido a tratamiento (informatizado o no) datos personales por quienes están involucrados en dicho tratamiento. Para concretar las denominadas Agarantías adecuadas@, contra los riesgos tales como, la pérdida de datos (que incluye el borrado a causa de accidente, la destrucción de soportes de información y el Ahurto@ de tales soportes), el acceso no autorizado para destruir, modificar o divulgar datos, o más aún, el uso indebido o no autorizado de los mismos (que incluye la reproducción no autorizada de datos), deberán las autoridades competentes implementar medidas idóneas proporcionales a los riesgos que los titulares de los datos pueden sufrir.

El grupo de expertos de la Recomendación de la OCDE, a título de ejemplo, propuso una serie de Agarantías adecuadas@, tales como, las de índole material (cerrojos en puertas y tarjetas de identificación, por ejemplo), *medidas de organización* (niveles jerárquicos en relación con el acceso a los datos, así como la obligación que tiene el personal responsable del tratamiento de la información de *respectar el carácter confidencial de los datos*), y sobre todo en los sistemas informáticos, *medidas relacionadas con la información* (encriptación, control de actividades inusitadas capaces de constituir un peligro y medidas tendentes a hacerles frente). (M.E. núm. 56).

6. El *Principio de transparencia*. Deberá adoptarse una norma general de transparencia en cuanto a las innovaciones, prácticas y criterios existentes con respecto a los datos personales. Deberá ser posible disponer fácilmente de medios que permitan determinar la existencia y naturaleza de los datos personales, el fin principal de su uso y la identidad del responsable de los datos y la sede habitual de sus actividades (R.12).

Como lo expone el grupo de expertos de la OCDE, el principio de transparencia puede ser considerado como condición previa del principio de participación individual. Como tal se considera una condición *sine qua nom*, para que pueda darse cabal y recto cumplimiento a uno de los principales principios con relación al tratamiento de datos, cual es el de la participación individual.

7. El *Principio de participación del individuo*. Toda persona física gozará de los siguientes derechos: 1) obtener del responsable del fichero o de otra instancia la confirmación de si el responsable de datos tiene datos acerca de su persona. 2) Requerir que se le comuniquen los datos que hicieren referencia a la misma, y ello: i) dentro de un plazo prudencial, ii) previo abono, en su caso, de una tasa que no fuere excesiva, iii) de manera razonable, iv) de manera directamente inteligible. 3) ser informado de la motivación de la resolución denegatoria de la petición formulada al amparo de los apartados *a*, y *b*, y poder recurrir contra la denegación. 4) impugnar datos que hicieren referencia a la misma y, en el supuesto de que la impugnación fuere fundada, requerir que los datos fueran cancelados, rectificados, completados o modificados (R.13).

Este principio fundamental esta estructurado por una serie de derechos y deberes que tienen y deben cumplir los sujetos interactuantes en el tratamiento o procedimiento (informatizado o no) de la información o datos. En efecto, se establecen los derechos que goza toda persona física en el transcurso del tratamiento de datos desde la recolección misma, así como las obligaciones que tienen que

cumplir los responsables del fichero o autoridades competentes para proteger, respetar y hacer respetar esos derechos. Todo ello, dirigido a garantizar la protección de la intimidad y las libertades individuales.

Cuando en el principio se hace mención a los derechos que tiene toda persona para acceder, conocer, impugnar, y en su caso solicitar, la cancelación, rectificación, complementación o modificación y actualización de los datos personales que le conciernen, simple y llanamente estamos haciendo referencia al derecho denominado de A*habeas data*@, por el cual la persona puede tener control de sus propios datos. Obviamente este derecho, como todo derecho fundamental, no es absoluto y está sometido a limitaciones previstas en las propias normas jurídicas.

Por ello, los expertos de la OCDE, concretaron lo siguiente:

a) El derecho de acceso deberá ser, en general, fácil de ejercitar. Esto puede significar, entre otras cosas, que debería formar parte del conjunto de las actividades cotidianas del responsable del fichero o del que hiciere sus veces y no requerir proceso judicial o medida análoga alguna. En algunos casos podría quizá ser conveniente prever un acceso intermedio a los datos; así, por ejemplo, en la esfera médica el médico podrá servir de intermediario.

b) La condición de que los datos sean comunicados dentro de un plazo razonable puede ser cumplida de modos diversos. Así, el responsable de un fichero que facilite información a los interesados a intervalos regulares puede ser dispensado de la obligación de responder inmediatamente a las peticiones formuladas individualmente. Normalmente, el plazo deberá ser computado desde la recepción de una petición. Su duración podrá variar en cierta amplitud de una situación a otra en función de circunstancias tales como la índole del tratamiento de la información.

c) La comunicación de tales datos *de manera razonable* significa, entre otras cosas, que debe presentarse la debida atención a los problemas de la distancia geográfica, cuando menos.

d) El derecho a ser informado de las razones, en los términos previstos en el apartado 3, es limitado en cuanto que se constriñe a situaciones en las cuales hubieren sido desestimadas peticiones de información.

e) El derecho a impugnar, contemplados en los apartados 3 y 4, tiene una gran amplitud, y comprende las reclamaciones formuladas en primera instancia ante los responsables de los datos y asimismo los subsiguientes recursos presentados ante tribunales, organismos administrativos, órganos profesionales u otras instituciones, siguiendo los cauces previstos en los reglamentos internos de procedimiento. El derecho a impugnar no implica que el interesado pueda decidir cuáles sean los recursos o reparaciones disponibles (rectificación, incluso de una anotación que precise que los datos son objeto de litigio, etc.); tales cuestiones serán resueltas aplicando el Derecho interno y los cauces procesales internos (M.E. núms. 58 a 61).

8. El *Principio de responsabilidad*. El responsable del fichero deberá responder de la observancia de las medidas tendentes a dar cumplimiento a los principios que anteceden (R.14).

Este principio dirigido al responsable de los ficheros constituye el principal principio-deber de éste y principio-derecho de los titulares de los datos personales para demandar su efectividad. Este responsable no será dispensado de tales obligaciones ni siquiera cuando el tratamiento de datos es Allevado a cabo por su cuenta por un tercero, como una oficina de servicios, por ejemplo. Más aún, es probable deducir responsabilidad@ al personal de las oficinas de servicios, a los

usuarios dependientes y a otras personas. Por ello, las sanciones impuestas por incumplir la obligación de *confidencialidad* podrán afectar a todas las personas, físicas o jurídicas, encargadas del tratamiento de los datos de carácter personal (M.E.núm.62).

4.3.1.2.2. PRINCIPIOS DEL TRATAMIENTO DE DATOS EN EL AMBITO INTERNACIONAL: LIBRE CIRCULACION Y RESTRICCIONES LEGITIMAS.

Este grupo de principios que se concreta en el *Principio fundamental de la Libre circulación de los datos*, está previsto en la parte III, apartados 15 a 18 de la Recomendación de la OCDE. Decimos grupo de principios porque la Recomendación no deslinda uno a uno, como sí lo hace en el ámbito nacional, los principios aplicables al ámbito internacional. En los apartados mencionados se dan pautas que unidas concretan el principio fundamental que se quiere resaltar, el de la libre circulación de los datos. Sin embargo, no debemos olvidar que siendo la transferencia, flujo o movimiento de datos uno de los ciclos posibles del tratamiento de datos personales, es lógico pensar que a esta clase de información transmitida en el ámbito internacional se tengan que aplicar los principios generales para todo el tratamiento de la información, es decir, los que hemos comentado en el apartado anterior, para el nivel nacional. Esta tesis se ve reforzada en el texto de la Recomendación misma, pues Alos países miembros deberán tender a la formulación de unos principios en el plano interno e internacional que rijan el derecho aplicable en los supuestos de flujos internacionales de datos personales@ (R.22), debiendo tener en cuenta estos países Alas implicaciones que para otros países miembros tuvieran el tratamiento interno de datos personales y su reexportación@ (R.15).

Para conseguir la incardinación de dichos principios e implementar las medidas de seguridad necesarias a nivel internacional, Alos países miembros deberán adoptar las medidas razonables oportunas para que los flujos internacionales de datos personales, incluso el tránsito por un país miembro, sean ininterrumpidos y seguros@ (R.16); es decir, que deben estar protegidos contra los accesos desautorizados, la pérdida, destrucción, modificación o cancelación de datos. Esta protección debe extenderse a todos los datos personales, incluso a los A*datos en tránsito*@, o sea, aquellos que transitan de un país a otro sin ser utilizados o almacenados en éste con finalidades de posterior uso o consulta [161].

Todo ello, por cuanto a nivel interno, los Estados miembros de la OCDE, presentaban diferentes problemas que no podía resolver aisladamente y surgidos por la adopción de medidas que amparan a la persona con respecto al flujo o movimiento de datos personales a través de sus fronteras [162] . Además porque, este flujo había crecido, a la par con la creación de *bancos internacionales de datos* (entendiendo como tales, los conjuntos de datos almacenados para poder ser recuperados y para otros fines). Esto no sólo justificaba la necesidad de cooperación internacional entre los Estados para resolver estos problemas, para velar porque los procedimientos aplicables al flujo internacional de datos personales y la protección de la intimidad y de las libertades individuales sean seguros y compatibles con los de otros países miembros, sino que consecuentemente fundamentaba el *libre flujo de la información*, así como el grupo de principios que éste conlleva, pues hasta ahora la libre circulación de datos A con frecuencia debe ser mitigado en aras de la protección de datos y de las oportunas limitaciones con respecto a su colecta, tratamiento y difusión@ (M.E.7).

Se establece como regla general, la libre circulación de los datos personales, como un principio-derecho, no absoluto, y por tanto limitada en los siguientes casos:

(161) AEI compromiso general que se contempla en el apartado 16 deberá ser considerado, por lo que respecta a las redes de ordenadores, dentro del contexto del Convenio Internacional de Telecomunicaciones de Málaga-Torremolinos (25 de Octubre de 1973). En virtud de este convenio, los miembros de la Unión internacional de Telecomunicaciones (UIT), entre ellos los países miembros de la OCDE, acordaron entre otras cosas, adoptar las medidas oportunas para crear los canales e instalaciones necesarios con el fin de asegurar un intercambio rápido e ininterrumpido de las telecomunicaciones internacionales. A mayor abundamiento, los países miembros de la UIT acordaron adoptar todas la medidas posibles y compatibles con el sistema de telecomunicación empleado, con objeto de garantizar el secreto de la correspondencia internacional. En cuanto a las excepciones, los miembros se reservaron el derecho de suspender el servicio de las telecomunicaciones internacionales, así como el derecho de comunicar la correspondencia internacional a las autoridades competentes, con el objeto de garantizar la aplicación de su legislación interior o la ejecución de los convenios internacionales en los cuales fueren parte los países miembros de la UIT. Estas normas se aplicarán tan pronto como los datos fueren transmitidos por medio de las lineas de telecomunicación. Dentro de su contexto propio, las directrices constituyen un medio suplementario de garantizar que los flujos internacionales de datos de carácter personal tengan lugar sin interrupción y con plena seguridad@ (M.E.núm. 66).

(162) AOtras razones para completar la reglamentación del tratamiento de datos personales a nivel internacional, son: a) los principios en juego hacen referencia a ciertos valores que varios países ansían preservar y ver respetados; b) pueden contribuir a ahorrar gastos en la circulación internacional de datos; c) los países tienen un interés común en evitar la creación de enclaves en los cuales fuera fácil hurtarse al cumplimiento de las reglamentaciones nacionales internas relativas al tratamiento de la información@ (M.E.9).

a) Todo país miembro deberá abstenerse de restringir los flujos internacionales de datos personales que tuvieren lugar entre su territorio y el de otro país miembro, excepto en el supuesto de que este no observare sustancialmente las presentes directrices o cuando la reexportación de dichos datos permitiere soslayar la aplicación de su legisla- ción interna de protección de la intimidad y de las libertades individuales (R.17 *Ab initio*).

b) Todo país miembro podrá asimismo imponer restricciones con respecto a determinadas clases de datos personales para las cuales su legislación interna de protección de la intimidad y de las libertades individuales previere regulaciones normativas específicas basadas en la naturaleza de tales datos, siempre que el otro país miembro no les otorgare una protección equivalente (R.17 *In fine*). Con ello no se quiere que los países tengan regímenes de protección idénticos (en forma y fondo), sino que sus efectos puedan considerarse en esencia idénticos entre los Estados que intervienen en el movimiento de datos (Emisor/Transmisor de datos. Aunque la Recomendación utiliza una terminología iusmercantilista criticable de Importador/Exportador de datos).

c) Los países miembros deberán abstenerse de dictar disposiciones legales, formular directrices políticas o crear prácticas que, concebidas en nombre de la protección de la intimidad y de las libertades individuales, excedieren las exigencias de dicha protección y fueren por ello incompatibles con la libre circulación de datos personales a través de las fronteras (R.18). Sin embargo, esta restricción impuesta a nivel interno no significa que se limite la actividad legislativa de los Estados sobre flujos transfronterizos en el marco comercial, tarifas aduaneras, empleo y Aa otros factores económicos conexos que condicionan el tráfico internacional de datos@ (M.E.núm. 68).

4.3.1.2.3. EXCEPCIONES A LAS DIRECTRICES.

La regla general que se establece en la Recomendación para estructurar las excepciones a las Directrices, es la de que éstas constituyen en el ámbito de aplicación de los Estados Miembros de la OCDE, Apautas mínimas susceptibles de ser completadas con medidas adicionales de protección de la intimidad y de las libertades individuales@ (R.6).

Si bien, ni técnica ni jurídicamente la Recomendación *sin fuerza ejecutiva*, expone un listado de los supuestos que deben considerarse como excepciones, como se hace en las legislaciones a nivel interno, no debe desdeñarse el hecho de plantear unas pautas generales para su aplicabilidad, partiendo de la expuesta regla general. En efecto, se entiende entonces que las excepciones serán las mínimas posibles y deben darse a conocer al público por medios idóneos (p.e. publicación en diario oficial). Dentro de ese *exceptionis mínimum*, la Recomendación destaca tres supuestos genéricos: La Soberanía y la Seguridad nacionales y el orden público. Aspectos estos que en las diferentes legislaciones de los Estados, aún ahora, han sido definitivos para construir un sistema de excepciones, aún vigente.

El sistema de excepciones propuesto por la Recomendación no fue *númerus clausus* ni concentrado. Lo primero, por lo que se ha dicho anteriormente; y lo

segundo, por cuanto no sólo constituyen eventos de excepciones a la regla general del tratamiento (informatizado o no) de datos, ni a la aplicación de los principios que propenden por su protección y garantía, sino porque en el contexto de la Recomendación se exponen supuestos con el nombre de Alimitaciones@, Arestricciones legítimas@, etc., que en puridad jurídica constituyen casos de excepciones. Bástenos mirar las llamadas restricciones legítimas al flujo internacional de datos [163].

4.3.2. EL CONVENIO DE ESTRASBURGO DE ENERO 28 DE 1981.

Una armonización legislativa internacional en los Estados Europeos sobre la protección de los datos personales sometidos a tratamiento informatizado por medios idóneos, constituía la aspiración capital del Convenio 108 del Consejo de Europa de 28 de Enero de 1981. Esto es lo que se pretendió con el Convenio de Estrasburgo, y en efecto se logró. El Convenio Europeo de 1981, como también se le conoce, relativo a la *protección de personas en relación con el tratamiento automatizado de datos de carác-*

---

(163) Véase, aparte 4.3.2.12.2.

ter personal, fue ratificado por España el 27 de Enero de 1984, con lo cual a partir de allí perteneció a los Estados con leyes de protección de datos de la *segunda generación.* Este texto, aparte de constituir norma jurídica de derecho interno en España, por el ingreso al ordenamiento jurídico (art.96.1 CE) y ser un eficaz instrumento de interpretación de los derechos humanos, en lo referente al Auso de la informática@ (STC 254/1993, de 20 de Julio), ha servido de modelo normativo (en forma y contenido no muy fiel, como veremos) a la *Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española --LORTAD--*: L.O.5/1992, Oct. 29 [164].

En el Preámbulo del Convenio de Estrasburgo, se establecen las líneas directrices y programáticas para todos los Estados Miembros del Consejo de Europa, así como las posturas jurídicas a observar por los dichos Estados, respecto a la protección de los derechos y libertades fundamentales, en general, y al derecho a la intimidad (aunque conceptualmente se refiera a Ala vida privada@), en especial. Esta particularidad ha hecho que la protección en el tratamiento informatizado de datos personales sea inmediatamente identificada en su vulnerabilidad con el derecho a la intimidad, tal como lo hicieran otras normas comunitarias y estatales de protección de datos. Así mismo se confirmó varios postulados y principios previstos en la Recomendación de la OCDE de 1980, pero especialmente sobre la *Libre circulación de datos, la libertad de información y la conciliación y respeto mutuo de derechos y libertades fundamentales.*

Estas Directrices capitales son: a) Propender por una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; b) Ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; c) Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; y d) Reconociendo la necesidad de

---

(164) Las infidelidades de la LORTAD, hoy son causa de recursos de inconstitucionalidad como veremos al final de esta parte de la investigación. El autor destaca la inspiración de contenido del Convenio seguido por la LORTAD. ORTI VALLEJO. A. Ob. ut supra cit., pág. 17.

conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.

Muy a pesar de que el preámbulo en todo cuerpo normativo tiene efectos materiales y jurídicos vinculantes sobre el contexto o articulado, el Convenio prefirió pasar de reiterativo y volvió a plasmar estas directrices en forma resumida en el artículo primero, confirmando con ello la protección en el tratamiento

informatizado de datos personales de todos los derechos, libertades públicas e intereses legítimos, no única y exclusivamente el derecho a la intimidad.

El Convenio está dividido en siete capítulos, a saber: 1. *Disposiciones Generales*: Objetivo y fin, definiciones, y ámbito de aplicación; 2. *Principios fundamentales de la protección de datos:* Obligaciones de las partes, calidad de los datos, clases especiales de datos, seguridad de los datos, garantías complementarias para el interesado, excepciones y restricciones, sanciones y recursos, y ampliación de la protección; 3. *De los flujos internacionales*: flujos internacionales de datos de carácter personal y derecho interno; 4. *Del Mutuo Auxilio:*Cooperación entre las partes, asistencia a los interesados residentes en el extranjero, garantías referentes a la asistencia prestada por las autoridades designadas, desestimación de peticiones de asistencia, gastos y tramitación de la asistencia; 5. *Del Comité Consultivo:* Composición del Comité, funciones del Comite, procedimiento; 6. *De las Enmiendas:*Enmiendas; y, 7. *Cláusulas Finales:* Entrada en vigor, adhesión de estados no miembros, cláusula territorial, reservas, denuncia, y notificación.

De este variopinto contenido, abordaremos el análisis de los siguientes temas: a) Las definiciones nucleares en el tratamiento informatizado de datos personales y, b) Los principios y excepciones fundamentales en el tratamiento y circulación de datos .

4.3.2.1. DEFINICIONES NUCLEARES EN EL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES.

El *poder de la informática* desde la expedición del Convenio y mucho antes, hacía gravitar sobre los usuarios de los sectores públicos y privado la consiguiente responsabilidad social. En la sociedad moderna, gran parte de las decisiones que afectan a los individuos descansan en datos registrados en ficheros o bases de datos (v.gr. Nóminas, expedientes de seguridad social, historiales médicos, judiciales, policiales, etc.). En los años que siguieron a aquella época, el tratamiento informatizado de la información continuó imponiéndose en el ámbito administrativo y de gestión, entre otras cosas, a causa del abaratamiento de los costes del

tratamiento informático de los datos, de la aparición en el mercado de dispositivos de tratamiento inteligente y de la creación de nuevos sistemas de telecomunicaciones para la transmisión de los datos, tal como lo destacaba también la Memoria Explicativa del Convenio (M.E.).

Un cierto halo de temor que rondaba a los operadores jurídicos (abogados, jueces, administradores, etc) al aplicar cuerpos normativos jurídico-técnicos, como lo era el Convenio Europeo de 1981, inspiraba a los legisladores a implementar un capítulo preliminar que funcione como glosario técnico-jurídico que guía y orienta a los operadores jurídicos del Convenio. Así, se paliaba ese temor, que aún ahora subsiste en todas las normas que regulan el fenómeno tecnológico de la información y la comunicación (TIC), unido a la informática.

En tal virtud, el Convenio definió los siguientes términos nucleares en todo tratamiento informatizado de los datos: Datos personales, persona identificable, interesado, Afichero automatizado@, Atratamiento automatizado@ y Aautoridad controladora@, entre otros.

Los datos de carácter personal (o datos personales), se consideran cualquier información relativa a una persona física identificada o identificable ("persona concernida", como insiste el Convenio).

Se deduce de esta definición, que el concepto de *persona concernida*, a los efectos de determinar de identificación dentro de un procedimiento informatizado de datos, no solamente abarca los rasgos de identificación de la persona de carácter jurídico (como los registros de nacimiento, médico, etc, documento de identificación personal v.gr. Documento Nacional de Identidad DNI en España o Documento de Identidad Nacional DIN o Cédula de ciudadanía en Colombia, Pasaportes, etc), sino también de carácter físico interno v.gr. exámenes de sanguíneos, de líquidos humanos diferentes a la sangre (semen, orina, etc.), exámenes morfológicos (color de piel, facial, dentales, ópticos, de estatura, etc); o de carácter físico externo, con fotografías y huellas humanas y/o tecnológicas (códigos, password o firmas

digitalizadas). Estas huellas, se consideran como rasgos diferenciadores de una persona humana de carácter morfológico o tecnológico con incidencia jurídica.

Esta identificación del ser humano o de la Apersona concernida@ es la que a la luz del Convenio constituye el núcleo central del concepto de datos de carácter personal, muy a pesar de que se sostiene en la E.M., del Convenio, que Apersona identificable@, es aquella Apersona que puede fácilmente ser identificada@, sin necesidad de Aidentificación de personas por métodos complejos@ [165]. Quizá en aquella época en que surgió la norma europea, tal proposición pudiera ser válida parcialmente, pero hoy no, pues dicha identificabilidad de las personas, antes y ahora debe incluir métodos y procedimientos científico-técnicos idóneos, máxime si se refiere al tratamiento informatizado de datos personales --con o sin el consentimiento del titular--, que relacionan datos personales contenidos en documentos jurídicos, registros de estado civil, médicos, judiciales, económicos o financieros, etc, en todos los cuales para una debida identificación de la persona se debe emplear medios idóneos de tipo técnico-científicos irrefutables previos al asiento o registro informático o concomitante con éste.

Hoy, el ser humano tiene un derecho a *la identificación* sico-física, como persona humana dotada de cuerpo, mente e inteligencia, válido o validable en todo ámbito social, cultural, político, económico, y sobre todo jurídico o iusinformático. Por lo tanto, no se puede desdeñar ningún método científico-técnico para la plena identificación en todo procedimiento que tenga incidencia en el pleno ejercicio de los derechos y libertades fundamentales de una persona. El Convenio recoge este parecer cuando sostiene que su objetivo prioritario es Areforzar la protección de datos, es decir, la protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal que les conciernen@ (M.E.núm. 1).

El concepto de persona concernida también se extiende al de persona A*interesada@*, que el Convenio utiliza en varios artículos. Así, *interesado*, Aexpresa *la*

---

(165) Memoria Explicativa del Convenio 108 de 1981. M.E.núm.28. Compilados por HEREDERO HIGUERAS, Manuel. *LEGISLACION INFORMATICA.* Ed. Tecnos, Madrid, 1994, pág.570

idea según la cual toda persona tiene un derecho subjetivo sobre la información relativa a sí misma, aún cuando tal información haya sido reunida por otras personas (cfr. la expresión inglesa *data subjetc*) **[166]**

El A*fichero automatizado*@ o bancos de datos. Significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado. Aunque en la E.M., del Convenio eufemísticamente se dice que se prefiere el nombre de fichero al de Banco de datos, porque esta expresión se utiliza Ahoy en un sentido más especializado: el de un fondo común de datos accesibles a varios usuarios@**[167]**. Sin embargo, la diferencia hoy por hoy es simplemente terminológica y de origen idiomático (Banco de datos término anglosajón A*database*@ o, Fichero informatizado del término francés A*Fichiers*@).

Los Estados Miembros del Consejo de Europa eran conscientes de que día a día crecían por la irrupción de la tecnología TIC y la informática, maneras y formatos de recolectar y almacenar información de todo tipo (incluida las denominadas Apersonales@) con medios informáticos, electrónicos o telemáticos, y que se materializaban en los llamados ficheros o bancos de datos, por regla general. Eran también, conscientes de que los diversos Estados tenían en sus sistemas jurídicos regulaciones sobre el derecho a la intimidad de las personas, la responsabilidad civil, el secreto o la confidencialidad de ciertas informaciones sensibles, etc. Sin embargo, se echaban de menos unas reglas generales sobre el registro y la utilización de informaciones personales y en Aespecial, sobre el problema de como facilitar a los individuos el ejercicio de un control sobre informaciones que, afectándoles a ellos, son colectadas y utilizadas por otros@ (M.E.núm.3). En tal virtud, se decidió concretar además de el concepto de datos de carácter personal, qué debe entenderse por fichero o banco de datos para proteger los derechos y libertades fundamentales de la persona y facilitar el autocontrol de los mismos por parte de la persona concernida.

El concepto de fichero o banco de datos informatizados, comprende Ano solamen-
te ficheros consistentes en conjuntos compactos de datos, sino a si mismo conjuntos de

---

(166) Ibídem., pág. 570.

(167) El M.E.núm. 30 ab initio, sostiene que la Aexpresión ´fichero automatizado´ ha sustituido a la de ´banco de datos electrónico´ utilizada anteriormente en Resoluciones (73)22 y (74)29 y en algunas leyes nacionales. Por ello, en el transcurso de la investigación utilizaremos indistintamente fichero o banco de datos para referirnos al mismo concepto.

datos dispersos geográficamente y reunidos mediante un sistema automatizado para su tratamiento@ (M.E.núm. 30 *ab initio*).

La definición de fichero Aautomatizado@ para diferenciarlo del fichero o banco de datos mecánico o manual, resulta reiterativo cuando menos desde el punto de vista terminológico, cuando al final sostiene que ese conjunto de informaciones deben estar sometidas a un tratamiento igualmente Aautomatizado@ (que mejor sería decir informatizado [**168**]). Sin embargo, esta observación es de menor entidad, frente a la significancia de la inclusión de un término imprescindible en el tratamiento lógico de entrada (E/) y salida (/S) de información por medios informáticos, como lo es el de fiche- ro o banco de datos informatizados. Esta aclaración delimita a su vez, el ámbito de aplicación del Convenio, al tratamiento informatizado de los datos o información de carácter personal, a diferencia de la Recomendación de la OCDE de 1980, que abarcaba incluso el tratamiento no informatizado de datos personales, aunque la definición siguiente desmienta tal diferenciación, al menos en toda su integridad.

En efecto, por *"tratamiento automatizado",* se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión (art. 2, c). Este tratamiento de datos se extiende a los datos de carácter personal en los sectores público y privado (art. 3-1, del Convenio) [**169**] .

(168) Preferimos decir Ainformatizado@, porque entre otras razones que se dan a lo largo de la investigación, existen estrechos vínculos entre la información obtenida (cualquiera sea esta, y más si es de tipo personal) con Ala informática documental@, según los términos del profesor *LOPEZ MUÑIZ-GOÑI,M* (En: Informática Jurídica Documental) que utiliza métodos y procedimientos informatizados en el tratamiento lógico, sistemático y analítico de la información que ésta proporciona y no solamente un tratamiento robótico o Aautomático@ de la información, tal como lo hacen los cajeros electrónicos, sistemas electrónicos de detección de personas o cosas, etc. Es un tratamiento logicial con medios informáticos, electrónicos o telemáticos y no simplemente cibernético o robótico aunque éste sea la base del mismo.

(169) El Convenio se aplica al sector público y privado. ASi bien es cierto que la mayor parte de la circulación internacional de datos tiene lugar dentro del marco del sector privado, el convenio reviste, no obstante, gran importancia para el sector público y ello por dos razones: en primer lugar, el art. 3 impone a los Estados miembros la obligación de aplicar los principios de la protección de datos aun en el caso del tratamiento de ficheros públicos --que es el supuesto normal-- totalmente dentro de sus fronteras nacionales. En segundo lugar, el convenio ofrece asistencia a los interesados que deseen ejercer su derecho a ser informados del registro que de ellas lleve una autoridad pública en un país extranjero. La distinción sector público- sector privado no aparece en las demás disposiciones del convenio, sobre todo porque esta nociones pueden tener significados distintos de un país a otro...@ (M.E.núm. 33)

Las acciones de tratamiento lógico de la información, que se traducen en fases o ciclos informatizados, según la definición de tratamiento automatizado del Convenio puede efectuarse total o parcialmente con procedimientos informáticos, con lo cual se introducen métodos de tratamiento mixtos de la información, en los cuales participan acciones mecánicas o manuales e informáticas.

El concepto técnico-jurídico abierto de *tratamiento de datos personales*, abre la posibilidad a la interpretación de que el Convenio no sólo regule el tratamiento informatizado de la información, sino también el no informatizado siempre y cuando contenga alguna parte, acción o fase de carácter informática. Esto es posible cuando la fase inicial o de recolección de información en un tratamiento lógico o informatizado es carácter mecánico o manual **[170]**.

Las fases o ciclos del tratamiento informatizado, según el Convenio se inician con el *registro de datos* y frente a él todas las acciones (u Aoperaciones aritméticas@, guar- dando con ello más relación al tratamiento robótico de la información que al lógico o sistémico) subsiguientes que pueden realizarse: modificación, borrado, extracción o difusión de la información **[171]**. Todas estas acciones a excepción de la última, son componentes de una acción eminentemente

tecnológica realizable con los datos (o Afiles@: archivos o registros), más que jurídica; puesto que, sí se quería referir a las acciones técnico-jurídico realizables con cualquier tipo de datos, debió hacerse mención a las fases de recolección, almacenamiento, registro, conservación, rectificación, bloqueo y cancelación de la información, tal como lo hiciera la LFAPD de 1977 [172], y posteriormente, la Recomendación de la OCDE de 1980.

Sin embargo, el contexto del Convenio aclara la deficiente definición de *tratamiento automatizado*, cuando se refiere: a) a los principios y derechos que tiene toda persona cuando han sido sometidos a tratamiento informatizado los datos personales

---

(170) Véase, parte III, *in fine*, sobre el procedimiento informatizado de datos personales en su fase in del tratamiento.

(171) La voz Adifusión@, según la E.M.núm. 31 ab initio,@ es un término genérico que abarca tanto la revelación de información a una persona (o a varias personas), como la consulta de la información por tales personas@

(172) Veáse, aparte 4.2.1. y ss, Parte I.

que le conciernen y, b) al hacer mención expresa a la fase de recolección (en los artículos 5-a y 12 del Convenio [173]) y de transmisión Ainternacional@ (o fase de comunicación) de datos, como fases ineludibles y/o posibles del tratamiento informatizado o no de datos. Esto a pesar de la insistencia de la E.M., núm. 31 *ab initio* del Convenio al excluir la fase de recolección o colecta de información Ade la noción de tratamiento@ de datos, con unos argumentos poco convincentes [174].

La *Autoridad "controladora del fichero"*,se considera a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero informatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les deberá aplicar.

La definición contiene un concepto ampliado del *ente almacenante* que trae la LFAPD, en el art. 1-1., y a la vez, una conceptualización casi idéntica a la de

Aresponsable del fichero@ contenida en la Recomendación de la OCDE de 1980, art.1-a. En efecto, la entidad almacenante atribuible a cualquier persona, entidad, servicio o institución pública o privada, tiene como función primordial el almacenamiento (que incluye según la ley alemana, las fases de recolección, registro y conservación) de datos por sí mismo o por encargo a otro. En cambio, Ael responsable del fichero@, tanto en el la Resolución de la OCDE, como en el Convenio 108 de 1981, abarca otros ciclos o fases como funciones del tratamiento informatizado de los datos o informaciones personales, tales como la transmisión de datos, la determinación de la finalidad del fichero, la categorización de los datos, el registro y hasta Acuáles operaciones se les aplicarán@ (art. 2, d), del Convenio), respectivamente.

---

(173) El Convenio utiliza los términos Aobtener@ o Areunir@, para hacer mención a la fase inicial de recolección o colecta de datos. En efecto, el art. 5, a), expresa: ALos datos de carácter personal que sean objeto de un tratamiento automatizado: a) *Se obtendrán* y tratarán leal y legítimamente@, y el Art.12., al referirse a los AFlujos transfronterizos de datos de carácter personal y el derecho interno : 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado *o reunidos* con el fin de someterlos a ese tratamiento@.

(174) Se dice que Aante el rápido desarrollo de la tecnología del tratamiento de la información, se consideró con- veniente enunciar una definición bastante general de Atratamiento automatizado@, susceptible de una inter- pretación flexible@.Y según, la autointerpretación del legislador comunitario del Convenio, la colecta queda excluida del concepto Atratamiento@.

El *Responsable del fichero* se diferencia en uno y otro cuerpo normativo (OCDE y Convenio) en la circunstacia de que el Aresponsable del fichero@, en el Convenio es única y Aexclusivamente la persona o ente que en última instancia responde de la gestión del fichero, pero no aquellas otras personas que llevan a cabo las operaciones del tratamiento de conformidad con las instrucciones del responsable del fichero@ (M.E.núm.32).

Este concepto de *Responsable del fichero*, cuando menos, determina dos aspectos importantes en el tratamiento informatizado de datos: por un lado, la exclusión de cualquier grado o nivel de responsabilidad de los que realizaran actividades de tratamiento por encargo; y de otra, que la determinación del

responsable del fichero, lleva aparejada una garantía para las personas concernidas con el tratamiento de datos personales, la cual es, que puedan en todo momento identificar plenamente al responsable del fichero [175].

4.3.2.2. PRINCIPIOS Y EXCEPCIONES FUNDAMENTALES EN EL TRATAMIENTO Y CIRCULACIÓN DE DATOS .

El Convenio 108 del Consejo de Europa de 1981, sobre protección de las personas en relación con el tratamiento informatizado de datos personales, no sólo Arefuerza@ la protección jurídica de los individuos en relación al tratamiento informatizado de información de carácter personal, tal como se prevé en el preámbulo, la E.M., núm. 1, y en el propio texto (art. 1); sino que además propone una armonización normativa en el ámbito competencial del Consejo de Europa. Quizá uno de los aspectos capitales en los cuales el Convenio más apuesta por la armonización normativa a nivel europeo, es precisamente en la estructuración de los principios y excepciones fundamentales, así como en los derechos subsecuentes para los titulares de datos personales que de aquellos se derivan. En efecto, el Convenio persigue homogeneizar

---

(175) En efecto, el art. 8., del Convenio 108 de 1981, al hacer referencia a las denominadas AGarantías complementarias para la persona concernida@, sostiene que cualquier persona deberá poder: Aa) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como *la identidad* y la residencia habitual o el establecimiento principal de *la autoridad controladora del fichero.*

todo lo atinente a la regulación de la protección de los titulares de los datos prevista en las leyes protección de aquellos dictados hasta ese entonces (v.gr.Alemania, Suecia, Suiza, Francia, Noruega, Luxemburgo, Portugal, etc), como también aquellas otras leyes que se dictaron a su amparo y guía, como es el caso de la Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española (L.O. 5/1992, de 29 de Oct.).

En efecto, las Comisiones y subcomisiones encargadas del estudio, análisis y proposición del texto definitivo del que luego fuera el Convenio Europeo de 1981,

reestructuró los principios inmersos en las leyes europeas de protección de datos y en forma mancomunada abordó la tarea de su proposición final con el grupo de expertos del Comité respectivo de la OCDE [176] . Especial atención le dedicó a los principios de la libre circulación y seguridad de los datos [177] . Quizá por ello, los principios como excepciones al tratamiento informatizado de datos personales en uno y otro cuerpo normativo comunitarios resultan coincidentes, con la diferencia de que en el Convenio de Estrasburgo, estos y aquellas tienen una especial regulación que los convierte en la columna vertebral del tratamiento informatizado de datos personales.

En efecto, el Convenio Europeo como regla general establece que los principios y excepciones al tratamiento informático de datos, rigen en todo el tratamiento o procedimiento informatizado de datos personales y no en forma exclusiva y/o excluyente de una fase o etapa de dicho tratamiento (v.gr. recolección, almacenamiento, registro, conservación, etc.). Así se deduce de la redacción dada a los arts. 5 a 9 del Convenio. El sistema de principios y excepciones están ligados entre sí, pues unos y otros tienden a garantizar y proteger los derechos, libertades públicas, intereses legítimos Ay los valores fundamentales en una sociedad democrática@ (M.E.núm. 55).

---

(176) M.E.núm. 14, ACooperación con la OCDE y con la CEE@.

(177) M.E. núm. 16. ALa comisión de las Comunidades Europeas, que ha llevado a cabo estudios sobre la armonización de las legislaciones nacionales dentro del marco de la Comunidad con relación a los flujos internacionales de datos y las posibles distorsiones de la concurrencia, así como sobre los problemas vinculados a la seguridad de los datos, mantuvo estrecho contacto con el Consejo de Europa.@

Es aquí donde halla eco y sentido el denominado A*núcleo irreductible*@[178] , basado en la catalogación de los principios y excepciones fundamentales del tratamiento informatizado de datos personales, con capitales fines y objetivos de protección y garantía de derechos y libertades fundamentales (no sólo el derecho a la intimidad, como se ha generalizado), el debido y oportuno cumplimiento que los

Estados deben observar en la implementación en el ordenamiento jurídico interno (es decir, armonización legislativa) y la reducción al mínimo de los posibles conflictos de las leyes o de jurisdicción.

4.3.2.2.1. PRINCIPIOS FUNDAMENTALES EN EL TRATAMIENTO Y TRANSMISION DE DATOS PERSONALES.

Ahora bien, hagamos referencia a los principios en relación con las fases del tratamiento informatizado de datos que es donde tienen aplicabilidad y vigencia.

4.3.2.2.1.1. FASE DE RECOLECCION DE DATOS.

En la *fase inicial o de recolección de los datos personales,* son aplicables los principios siguientes: a) De lealtad y legitimidad (art.5-a,); b) De Prohibición excepcionada a la recolección de datos pertenecientes al Anúcleo duro de la privacy@ anglosajona [179] (art. 6); y, c) De información en la recolección, sobre los objetivos y fines de la misma (art. 8).

Estos principios se hallan en el Convenio bajo los epígrafes de Acalidad de los datos@, Acategorías particulares de los datos@ y Agarantías complementarias para la persona concernida@.

---

(178) Institución de derecho público que se explica en relación con los principios y *per se.* En efecto, Alos principios del ´núcleo irreductible´ reconocen a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento automatizado de datos de carácter personal@ (M.E.núm. 20 *in fine*).

(179) Comentado por el profesor MORALES PRATS, Fermín. *COMENTARIOS A LA PARTE ESPECIAL DEL DERECHO PENAL*. En: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Ed. Aranzadi, Pamplona, 1996, pág. 310 y ss.

El principio de lealtad y legitimidad, como principio de causa y efecto entre el objeto del tratamiento (datos) y su actividad (recolección), se entiende que los datos que se van a obtener, recoger o recolectar debe pertenecer a una persona

identificada o identificable, procesarse con métodos informáticos idóneos que permitan no vulnerar los derechos y libertades fundamentales del titular de los mismos y se proceda de conformidad con el ordenamiento jurídico vigente en cada Estado y en concordancia con las normas comunitarias. Queda proscrita toda recolección de datos en forma ilícita, ilegítima, indebida, inoportuna o expresamente prohibida. Quizá por esto último resulta incompleta la calificación de este principio como Aprincipio de legalidad@ de los datos, que algún sector de la doctrina ibérica lo nomina (*Castells*, *Souviron*, *López*, etc), pues la ley queda transvasada, cuando se involucra el interés estatales o personal, el criterio de la oportunidad del tratamiento, etc.

En principio, está prohibida la recolección de datos de carácter personal denominados Asensibles@ [180] que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales (art. 6) [181].

4.3.2.2.1.2. FASE DE ALMACENAMIENTO DE DATOS.

En *la fase de almacenamiento* de datos, serán aplicables los principios de: a) Exactitud del contenido (o Averacidad@, según *Souvirón* [182]) y de sujeción a la revisión y actualización (art. 5-d); b) De prohibición excepcionada de los datos denominados Asensibles@ (art.6); y c) De información en el almacenamiento de datos sobre los objetivos y fines del mismo (art. 8).

---

(180) Según *E. Vilariño*, datos sensibles son Aaquellos datos personales que se refieren a las características morales o físicas que, en principio, no son de interés para los demás y no afectan en general a la sociedad y cuyo conocimiento, en cambio, puede perjudicar injustificadamente los derechos e intereses legítimos de esas personas@, p. 54. Citado por SOUVIRON, José M. *EN TORNO A LA JURIDIFICACION DEL PODER INFORMATICVO DEL ESTADO.* R.V.A.P.Núm. 40, Sep-Dic., Bilbao, 1994, cita núm. 67 pág.153.

(181) Sobre el particular ahondaremos en su tratamiento en la Parte III y IV., de esta investigación. Por ello, re- mitimos a lo allí sostenido.

(182) SOUVIRON, José M. Ob. cit. ut supra. pág. 152.

4.3.2.2.1.3. FASE DE REGISTRO DE DATOS.

En la *fase de registro de los datos personales*, que es la etapa sobre la cual más incide el Convenio Europeo, quizá por las implicaciones de tipo socio-jurídico que se derivan de dicha actividad informatizada de datos, pues ésta sobreviene con carácter definitivo en tanto no haya causas para suspenderla, suprimir o cancelarla de conformidad con el ordenamiento jurídico vigente. Pareciera , por la redacción inicial del Convenio que la protección de los titulares de los datos se inicia con el registro de los mismos y no antes. Sin embargo, una recta interpretación del Convenio extiende la protección al momento mismo de la recolección de datos, haciendo énfasis en la etapa del registro porque supuestamente más afloran los síntomas de vulnerabilidad, aspecto éste que es más apariencia que realidad, como se ha visto.

Los principios aplicables a esta etapa del tratamiento informatizado son: a) De compatibilidad de las finalidades (art. 5-b); b) De adecuación, pertinencia y no excesibilidad de las finalidades (art. 5-c); c) Prohibición excepcionada del registro de datos personales denominados Asensibles@ (art.6); d) Principio de información en el registro de datos (art. 8); y . e) Principio de ASeguridad de los datos@ (art. 7).

Se destacan en esta etapa los principios de información y seguridad de los datos, por cuanto, en puridad jurídica es aquí donde nace el derecho de *habeas data* [183] y los subsecuentes derechos que este conlleva. Efectivamente, tras el ejercicio el derecho de la información y conocimiento por parte del titular de los datos, de terceros, de personas autorizadas o no, las personas naturales, jurídicas, públicas o privadas encargadas del tratamiento (o responsables) de datos toman las necesarias medidas de seguridad para la protección de datos de registrados en ficheros informatizados, a fin de evitar la destrucción accidental o no autorizada, la pérdida accidental o el acceso, la modificación o la difusión no autorizados.

---

(183) Se considera un derecho fundamental, que según *Fairen Guillen*,@ ya no (solo) es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data* Tales son las ideas generalmente admitidas hoy entre juristas y en el Derecho comparado, que

ofrece una de las vías para determinar el contenido esencial de un derecho fundamental (S.T.C. 11/1981)@ en el derecho español. Cfr. FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL SUGERIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992.* En: Revista de Derecho Procesal. Núm.3, Madrid, 1996, pág.530.

En tal virtud, aquí se ponen en juego las que el Convenio en el artículo 8, llama AGarantías complementarias para la persona concernida@, dentro de las cuales cualquier persona podrá: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos de Acalidad de los datos@ y Acategoría particular de datos@; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, luego de conocer la existencia de un fichero con los datos del concernido o de obtener a Aintervalos razonales@ la confirmación de tal existencia o no.

4.3.2.2.1.4. FASE DE CONSERVACION DE DATOS.

En la *fase de conservación de los datos,* se aplicará los siguientes principios: a) De identificación del concernido y de compatibilidad de las finalidades. En ejercicio de este principio, se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado (art. 5-e,); b) De Prohibición excepcionada en la conservación de datos personales considerados Asensibles@ (art.6); c) De Seguridad de los datos (art. 8); y d) De información en la conservación de datos.

4.3.2.2.1.5. FASE DE TRANSMISION DE DATOS. EN PARTICULAR, EL AFLUJO INTERNACIONAL DE DATOS@ [184] .

---

(184) La M.E.del Convenio Europeo Aespecifica el alcance de la noción de *flujos internacionales*, ha sido redac- tado de tal manera que tenga en cuenta la gran diversidad de los factores determinantes del modo en que los datos son transferidos: modalidad de representación (texto libre o codificado), soporte (papel, tarjeta perforada, cinta perforada, cinta magnética, disco, etc), medio de transporte (transporte físico, correo, enlace de telecomunicación conmutada por circuito o paquetes), interfaz (ordenador con terminal, ordenador con ordenador, manual con ordenador, etc), el circuito dedicado (directo desde el país de origen al país de destino, o a través de uno o varios países de tránsito), las relaciones entre el emisor y el destinatario (pertenecientes ambos a una misma organización o a distintas organizaciones), etc. (M.E.núm. 63). El tema será vuelto a tratar en la parte III y IV de esta investigación.

En la *fase de transmisión, flujo o movimiento de los datos*, a la que el Convenio también le ha prestado especial cuidado y tratamiento, rigen los principios previstos bajo los epígrafes de Acalidad de datos@, Acategoría particular de datos@, ASeguridad de datos@ y Agarantías complementarias para la persona concernida@, que antes hemos referenciado, pues al fin y al cabo la transmisión de datos es otra fase más del tratamiento de datos, tal como lo sostiene el art. 12.1 del Convenio Europeo [185]. Pero además, se aplicará un principio fundamental y específico para esta fase del tratamiento informatizado de datos personales, cual es la A*libre circulación de datos*@[186], que desde la Recomendación de la OCDE de 1980, ya había sido planteado y sustentado.

Esta fase del tratamiento informatizado de datos personales es tan importante como delicada, pues los Estados que poseían medidas legislativas protectoras de dicho tratamiento habían preparado y aplicado sus normas hacia el interior de sus zonas geográficas, pero no estaban preparados inicialmente para afrontar los dificultades sobrevenidas por la transferencia de datos entre Estados. La creación de Abancos de datos internacionales@, con diferentes fines, objetivos y actividades evidenció más aún dichas dificultades, pero a la vez, con la generalización de las transferencias internacionales en los ámbitos sociales, políticos, culturales, jurídicos y sobre todo económicos de la UE, se puntualizó y potenció toda clase de medidas

de seguridad, eficacia, oportunidad y celeridad de la transmisión/emisión de datos personales, para eliminar las dificultades y aumentar el flujo necesario de información entre Estados, sin mayores riesgos que los sobrevenidos de actividades indebidas, ilegales o no autorizados, tanto de tipo técnico como jurídico. En efecto, así ocurrió con las variopintas transacciones comerciales (v.gr. agencias de viajes, operaciones bancarias, cajeros automáticos: tarjetas de crédito, debido, etc.), las transferencias en actividades personales privadas o públicas (.v.gr. Bancos de datos médicos, investigativos, bibliotecológicos, estadísticos, etc); o en fin,

---

(185) Artículo 12. Flujos transfronterizos de datos de carácter personal y el derecho interno 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal *que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento@* (Cursivas nuestras).

(186) Este principio fundamental en el tratamiento y transmisión de datos personales, tanto para los individuos como para los Estados, se erigió, Ahabida cuenta de la rápida evolución de las técnicas de tratamiento de la información y del desarrollo de la circulación internacional de datos...(y de que era) conveniente crear unos mecanismos a escala internacional que permitan a los Estados tenerse informados mutuamente y consultarse entre sí en materia de protección de datos@ (E.M. núm. 11 *in fine*).

para transmitir información de un lugar geográfico transfronterizo a otro sin las debidos controles (técnicos o jurídicos, según la M.E.núm. 8), con fundamento en los adelantos de las telecomunicaciones, la informática, o la unión de las dos: la comunicación electrónica o telemática.

En especial, --se decía en el E.M.núm.9-- existe el temor de que los usuarios se sientan tentados a Ahurtarse@ a los controles impuestos por la protección de datos desplazando sus operaciones, en todo o en parte hacia Aparaísos de datos@, es decir, a países que tengan leyes de protección de datos menos rigurosas o que carezcan de leyes de protección de datos. Aunque algunos otros Estados para evitar estos riesgos han previsto en su Derecho interno controles jurídicos especiales, como las Aautorizaciones de exportación de datos@, las cuales pueden resultar excesivos o insuficientes, frente a la avalancha de crecimiento de las transmisiones electrónicas de datos entre Estados.

El Convenio, en consecuencia, establece que un Estado no podrá Aprohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter

personal con destino al territorio@ de otro Estado, so pretexto Ade proteger la vida privada@, salvo: a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación del otro Estado (*o Parte*) establezca una protección equivalente; b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otro Estado, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación del Estado a que se refiere el comienzo del presente párrafo (art. 12 *in fine*)..

En estas transmisiones interestatales, el mayor flujo de circulación de datos lo ocupan las transferencias de datos de carácter personal, por ello, el Convenio plantea como regla general, la *libre circulación de información* , como principio fundamental, tanto para los individuos como para los Estados (o Apueblos@, según la E.M.núm.9) y como excepciones, las directrices previstas con carácter de *numerus clausus* para algunas categorías de datos personales (básicamente los denominados *sensibles*) o ficheros que los contengan y para aquellas transmisiones triangulares entre Estados y uno de los cuales no pertenezca al Consejo europeo.

Si no fuese así, Atales controles (como el de la autorización, p.e.) podrían crear trabas a la libre circulación de la información@, erigida como principio fundamental en el tratamiento y transmisión de datos personales entre Estados. AHabía que encontrar, por tanto, una fórmula que garantizara que la protección de datos a escala internacional no vulneraría este principio@ (M.E. núm. 9 *in fine*). Se trata en últimas de conciliar [18 7] dos aspectos capitales en el tratamiento y transmisión de datos personales, que tienen la particularidad de ser concurrentes y aparentemente excluyentes: por un lado, la protección de datos; y por otro, la libre circulación de los mismos. Concurrencia que se consigue cuando toda transmisión o flujo de datos debe preveer cierto mínimo de garantías o de protecciones, pero no de controles especiales ni menos rigurosos que pudieran excluir la libre circulación de

los datos. De ahí el establecimiento de una regla general con sus taxativas excepciones.

La E.M., del Convenio sustenta una serie de características especiales referentes a los flujos internacionales de datos, las cuales en su conjunto reafirman la regla y excepciones anotadas.

En efecto, se establece que con base en el principio del *núcleo irreductible* que reconoce a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento informatizado de datos, y como tal, al obligarse a aplicarlos los Estados y miembros, Atienden a suprimir entre ellos las restricciones de los flujos internacionales de datos, evitando que el principio de libre circulación de datos sea puesto en tela de juicio por alguna forma de proteccionismo@ (M.E.núm. 20 *in fine*).

Respecto de la transmisión o flujos de datos personales calificados de sensibles

---

(187) Ese es el objeto principal del art. 12 del Convenio de Europa, Aconciliar las exigencias de protección eficaz de los datos con el principio de la libre circulación de la información independientemente de la existencia de fronteras, consagrado por el artículo 10 del Convenio Europeo de los Derechos del Hombre@ (E.M. núm. 62).

(relativos al origen racial, origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, la salud **[188]** o a la vida sexual, según el art. 6 del Convenio) se establece, al menos dos directrices para que un Estado justifique la derogación de las garantías que el Convenio ofrece a esta clase especial de datos personales. Estas son:

a) Cuando las medidas específicas de protección de tales datos fueren sensiblemente distintas de las disposiciones del derecho de los demás Estados que hicieren referencia a tales datos y, en especial, cuando tales medidas ofrecieren, de conformidad con el art. l1, (es decir, que ninguna de las disposiciones del capítulo II,

se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Estado, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio) un nivel de protección que transcendiere las normas mínimas contenidas en el Convenio.

b) Cuando determinados datos o ficheros que no estuvieren previstos dentro de los denominados datos sensibles, estuviesen sujetos a garantías especiales.

No será lícita la derogación, en estos casos, si el Estado destinatario ofreciere una protección equivalente. v.gr. Si un Estado somete los flujos internacionales de datos a una autorización especial, no puede negarse otro Estado, so pretexto de razones de protección de la intimidad, a conceder una tal autorización si el país receptor concede una protección equivalente (E.M. núm. 69 *in fine*).

Respecto de la *transferencias triangulares de datos personales*, o sea, aquellas que tienen lugar en dirección a un Estado no contratante a través de un Estado contratante, la derogación sólo puede ser invocada si está previsto que los datos transferidos se encuentren en un Estado contratante sólo en tránsito. No deberá ser invo-

---

(188) Los datos de carácter personal relativos a la salud, fue cuidadosamente estudiado por el Comité de expertos de protección de datos dentro del contexto de sus trabajos sobre los bancos de datos médicos. Tal noción abarca las informaciones concernientes a la salud pasada, presente y futura, física y mental, de un individuo. Puede tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas (E.M. núm. 45).

cada sobre la base de la mera presunción o expectativa de que los datos transferidos a otro Estado contratante pudieran, en su caso, ser transferidos a un Estado no contratante (E.M. núm. 70).

4.3.2.2.2. EXCEPCIONES AL TRATAMIENTO INFORMATIZADO DE DATOS Y A LOS PRINCIPIOS. LAS ARESTRICCIONES@.

Para establecer un régimen jurídico de excepciones en un ámbito interestatal, se debe tener en cuenta, al menos dos reglas primordiales: el objeto y fin de la norma jurídica y la taxatividad en la enunciación de los supuestos de excepciones. Todo ello, para que los Estados no Atropiecen con dificultades en cuanto a la interpretación de la excepción, pues ello podría obstaculizar gravemente la aplicación del Convenio@ (E.M.núm. 35 *in fine*).

Por lo primero, el Convenio Europeo, según el art. 1., establece que su objeto y fin es garantizar, en los territorios de los Estados miembros, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus *derechos y libertades fundamentales*, concretamente su derecho a la intimidad (o Avida privada@), con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").

Respecto de lo segundo, es decir, la regulación *numerus clausus* de los supuestos de excepciones, están previstas en el art. 9 del Convenio, con las siguientes anotaciones:

La regla general, para las excepciones al tratamiento informatizado de datos, consiste en la no admisión de excepción alguna contra los principios fundamentales previstos para las fases o etapas del tratamiento informatizado de recolección, almacenamiento, registro y conservación de datos personales, salvo que estuviere: prevista en el ordenamiento jurídico vigente del Estado miembro y constituya una medida necesaria en una *sociedad democrática*, para: a) la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; y, b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

Estas excepciones a la excepción de los principios fundamentales del tratamiento informatizado, están inspiradas en el Convenio Europeo de los Derechos del Hombre (arts. 6, 8, 10 y 11). Así mismo, la expresión Amedida necesaria@ en

una sociedad democrática, constituye una noción fruto de los acuerdos de la Comisión y el Tribunal de los Derechos Humanos, por la cual, resulta claramente que los criterios de tal concepto no pueden ser fijados para todos los Estados y en todo momento, sino que deberían ser considerados a la luz de la situación dada en cada Estado [189].

Las excepciones a la regla general tienen como fuente dos grandes ramales, a saber: los intereses fundamentales de los Estados y los intereses particulares de la persona humana.

En efecto, la enumeración taxativa dentro de las causales exceptivas al tratamiento y principios fundamentales de los datos obedece básica y exclusivamente a la delimitación conceptual de los que se consideran intereses principales de los Estados, es decir, de aquellas instituciones socio-jurídicas ; tales como, la seguridad del Estado [190], seguridad pública , intereses monetarios del Estado [191] e infracciones penales [192]; y por su puesto, a fin de evitar que en la aplicación del Convenio los Estados puedan tener un Amargen de maniobra demasiado amplio@ en la interpretación y aplicación de las mismas y conserven la facultad de Arehusar@[193] la aplicación del

---

(189) Las excepciones se limitan a las que son necesarias para proteger los Avalores fundamentales en una sociedad democrática@. (E.M.núm. 55).

(190) Se entiende por *Seguridad Pública*, en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado (E.M.núm. *56 in fine*).

(191) *Intereses monetarios del Estado*, comprende todo aquello que contribuye a facilitar al Estado los recursos financieros de su política. v.gr. La recaudación de los impuestos y al control de cambios. (E. M. núm. 57 *ab initio*).

(192) *Represión de los delitos*, comprende tanto la investigación de los delitos como su persecución (E.M. núm. 57 *in fine*).

(193) *Artículo 16. Denegación de peticiones de asistencia*. Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 (ACooperación entre Estados) o 14 (Asistencia a las personas concernidas que tengan su residencia en el extranjero) del presente Convenio, solamente podrá negarse a atenderla si: a) La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder; b) la petición no está conforme con lo dispuesto en el presente Convenio; c) atender a la petición fuese incompatible con la soberanía, la seguridad o el orden público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

Convenio en casos concretos por motivos de importancia ponderada (E.M.núm. 56).

En cuanto a la enunciación taxativa de las causales de excepción al tratamiento y principios básicos de los datos previstas en el literal b), sobre protección de la persona concernida están fundadas en los intereses particulares de la persona humana, tales como los del *interesado* (p.e., información psiquiátrica) o de *terceros* (p.e., la libertad de prensa, secretos del comercio, etc).

Conjuntamente con este marco de excepciones, el Convenio presenta las que llama Arestricciones@ al ejercicio de los ciertos derechos de la persona concernida y presentes en los Aficheros automatizados@ de datos personales que se utilicen con fines estadísticos o de investigación científica [**194**], cuando no existan manifiestamente riesgos de atentado a la intimidad (Avida privada@) de las personas concernidas (art. 9-3).

Jurídicamente están restricciones no se consideran excepciones, sino limitaciones al ejercicio de algunos derechos impuestas por razones expresamente previstas en el ordenamiento jurídico, y como tal, pueden ser preventivas (*in tempore*) o modales (eliminación del riesgo o vulnerabilidad). Sin embargo, en la *praxis,* estas restricciones pueden esconder verdaderas instituciones nugatorias de derechos, aún cuando fueren preventivas o modales.

Las restricciones al ejercicio de algunos derechos en las circunstancias y para ciertos ficheros o bancos de datos previstos en el Convenio, se extiende a aquéllos derechos de la persona concernida que como Agarantía complementaria@ ostenta en el transcurso del tratamiento informatizado de datos personales. Esos derechos son los componentes del derecho de *habeas data* que inicia con el de información. En efecto, se admite la restricción al ejercicio de los siguientes derechos: a) *De confirmación* de la existencia o no de un fichero con datos del concernido, así como el de comunicación de

(194) En los ficheros o banco de datos estadísticos la posibilidad de limitar el ejercicio de los derechos de los interesados, se centra en las Aoperaciones de proceso de datos que no llevaren aparejado riesgo alguno... en la medida en que se trate de datos presentados en forma agregada y separada de los identificadores. Igual los ficheros de datos científicos de conformidad con una recomendación de la Fundación Europea de la Ciencia (E.M.núm. 59 *in fine*).

dichos datos; b) *De rectificación* o borrado de datos, según fuere el caso, si se desconoce los principios fundamentales del tratamiento informatizado de datos (recolección, almacenamiento, registro y conservación) o la consideración de ser datos sensibles; y c) *De recurso*, ante las autoridades competentes, si no se atiende o se desconoce los anteriores derechos.

4.4. ESPAÑA: LEY ORGANICA DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL.

La Ley orgánica de regulación del tratamiento automatizado de datos de carácter personal, L.O. 5/1992, Oct. 29, (en adelante LORTAD) que entró en vigor el 31 de enero de 1993 (novísima ley que clama reformas) [195], no es en estricto rigor jurídico una ALey Española de informática@, como lo sostiene Fairen Guillen [196], a pesar de que se refiera a las etapas, principios, derechos-deberes y recursos del tratamiento informático de datos personales, ni tampoco es una ley orgánica que regula en forma plena el tratamiento informatizado de datos personales de titularidad pública y de titularidad privada, pues además de las excepciones *numerus clausus*[197], que deja por

---

(195) La LORTAD LO 5/1992, de 29 de Octubre, entró en vigor práctica como jurídicamente, el 31 de enero de 1993, puesto que la disposición final cuarta, expresamente sostenía que aquella se producirá tres meses después de la publicación en el Boletín Oficial del Estado (BOE 31-10-1992, núm. 262, [pág. 37037]). Terminaba así con la existencia de la disposición transitoria primera de la 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* y por la cual, se aplicaba la mencionada ley, aunque en un ámbito de comprensión legislativa y aplicabilidad hermenéutica restringidos (pues se refiere sólo Aa las intromisiones ilegítimas derivadas del uso de la informática) a todos aquellos aspectos referentes al tratamiento informatizado de datos personales, la protección de los derechos y libertades fundamentales e intereses legítimos y el uso de la informática, según lo estipuló la disposición única derogatoria de la LORTAD. La vida y derogación jurídicas de unas normas jurídicas que regulan el tratamiento informatizado de datos personales en España, estaba marcada no sólo temporal sino espacialmente de una etapa fructífera de cariz legislativo comunitario y estatal europeos en materia de protección de los titulares de los datos personales, más que de los datos *per se*, cuando son sometidos a procesos informáticos con soportes y medios informáticos, electrónicos o telemáticos, como hemos. Quizá esta sea una de las fundamentales razones para proponer reformas legislativas a la actual LORTAD y sus correspondientes Reales Decretos que la

reglamentan. Razones que al interior de España se han ampliado y plasmado en los variopintos recursos de inconstitucionalidad de la LORTAD, ante la Tribunal Constitucional Español, como veremos más adelante.

(196) FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL SUGERIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992*... Ob. ut supra cit., pág. 523 y ss.

(197) El régimen de protección de los datos de carácter personal que se establece en la presente LORTAD, no será de aplicación: a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general. b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales. c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales. d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales. e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación

fuera de su regulación ciertos tipos, categorías y clasificaciones de procedimientos informatizados, hace mayor incapie en el tratamiento informatizado de datos de carácter particular.

La LORTAD es una ley que persigue inicialmente la protección de la trilogía de derechos previstos en el art. 18.4 CE: el honor, la intimidad y la propia imagen Ay el pleno ejercicio de sus derechos@. Luego, en el contexto de la ley se hace se hace énfasis en la protección del derecho a la intimidad, por considerarlo el más vulnerable dentro del tratamiento informatizado de datos, pese a que en la praxis de nuestra *sociedad informatizada*, los nuevos fenómenos tecnológicos TIC y la informática, tienen como características su alta porosidad y penetrabilidad en todos los sectores de la vida humana. Sin embargo este énfasis de la LORTAD, es explicable pues por herencia temática, las anteriores leyes protectoras de datos desde las estatales de las década de los 70´s y 80´s, así como las normas internacionales (La Resolución de la OCDE de 1980) y las comunitarias europeas (Convenio 108/1981), concibieron sus leyes garantistas teniendo como núcleo el derecho a la intimidad, llamándolo indistintamente Aprivacy@, Avida privada@, Aprivacidad@, etc. Más aún, las nuevas leyes comunitarias europeas protectoras de los titulares de datos personales, como veremos, en forma expresa dirigen el ámbito garantísta en

forma casi exclusiva y excluyente hacia el derecho de la intimidad (Directiva 95/46/CE, Directiva 97/66/CE).

En el ámbito de la LORTAD, la protección enfatizada del derecho a la intimidad (o de la Aprivacidad@, según *Heredero Higueras y González Navarro,* aún cuando sólo en la E.M. núm. 1 y no en el texto de la norma jurídica se hace la distinción entre la

---

----Continuación nota 197---

el artículo 7 por tratarse de los datos personales en él contenidos. 3. Se regirán por sus disposiciones específicas: a) Los ficheros regulados por la legislación de régimen electoral. b) Los sometidos a la normativa sobre protección de materias clasificadas. c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes. d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36. e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio , Reguladora del Régimen del Personal Militar Profesional (Art. 2-2 y 2-3).

Aprivacidad@ y la Intimidad@ **[198]**. Distinción y alcances conceptuales que defiende *González Navarro* **[199]**) se plasma en el contexto de la norma jurídica, y sobre todo en la circunstancia de que el derecho a la intimidad es la principal fuente de inspiración del texto garantista de los demás derechos y libertades fundamentales que persigue proteger la LORTAD en todo tratamiento informatizado de datos, tal como lo revela un sector de la doctrina ibérica **[200]**.

Pese a ello, la LORTAD, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas

---

(198) A *Nótese que se habla de la privacidad y no de la intimidad*: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona --el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo--, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo. Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la

distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona. Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos -- datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado Adinero plástico@, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos-- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos@ (E.M. núm. 1). Texto completo en AA. VV. *COLECCION DE DISCOS COMPACTOS DE ARANZADI*. Ed. Aranzadi, Pamplona, 1997.

(199) Previa a la transcripción de la E.M.núm. 1., el autor manifiesta: AAunque suele pensarse que la protección de la privacidad tiene su fundamento en el derecho al honor y a la intimidad, y así parece resultar del artículo 18.4 , CE y de la misma exposición de motivos de la LORTAD que invoca expresamente este artículo, el verdadero fundamento de la específica protección de la privacidad se encuentra en el derecho al libre desenvolvimiento de la personalidad, un derecho que aunque no está específicamente mencionado en nuestra Constitución, es innegable que existe y está constitucionalmente protegido, como se prueba cuando se leen los artículos 14, 15, 16, 18.1, 20.1. b), 27.2, 38 y 44.1, todos los cuales pueden reconducirse a aquél@. GONZÁLEZ NAVARRO, Francisco. COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y PROCEDIMIENTO ADMINISTRATIVO COMUN (Ley 30/92)., Ed. Civitas S.A., Madrid, 1997, pág. 697-698.

(200) Así se deduce del tratamiento y análisis que los diferentes autores ibéricos hacen de la LORTAD. A título de ejemplo, ORTI VALLEJO, Antonio. DERECHO A LA *INTIMIDAD E INFORMATICA*... Ob cit., ut supra. SOUVIRON, José M. *EN TORNO A LA JURIDIFICACION*... Ob. cit., ut supra. FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL*... Ob. cit. SARDINA VENTOSA, Francisco. *EL DERECHO A LA INTIMIDAD INFORMATIVA Y EL TRATAMIENTO DE DATOS PERSONALES PARA LA PREVENCION DEL FRAUDE*. En: Actualidad Informática Aranzadi. Núm. 25, Oct, Pamplona, 1997. LOPEZ DIAZ, Elvira. EL DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD. Ed. Dykinson, Madrid, 1996.

y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas *y el pleno ejercicio de sus derechos* (art. 1); vale decir, del conjunto de derechos y libertades fundamentales previstos en la Constitución Española de 1978, aunque tanto en la praxis como en la teoría siga pesando el esquema de protección de la intimidad a través de las leyes protectoras de datos personales, y por su puesto, en la LORTAD.

Ahora bien, a nuestros efectos, analizaremos la visión iusinformática de la intimidad **[201]** tal y como hemos hecho con las demás normas relativas a la protección de los titulares de los datos. En tal virtud, abordamos y comentamos de la LORTAD, los siguientes temas: a) Las definiciones técnico-jurídicas; b) Los principios fundamentales aplicados a las fases del tratamiento informatizado de

datos personales; c) Los órganos de protección de los datos personales; y, d) Las Inconstitucionalidades de la LORTAD, que afectan al tratamiento y proceso informatizado de datos.

4.4.1. DEFINICIONES TECNICO-JURIDICAS APLICABLES AL TRATAMIENTO INFORMATIZADO DE DATOS.

Con los antecedentes legislativos europeos (Alemania, Suiza, Francia, etc.) y comunitarios (básicamente de la Recomendación de la OCDE de 1980 y el Convenio Europeo de 1981), el Estado Español introdujo en su ordenamiento jurídico, una legislación homogénea, pero no plena en el tratamiento (informatizado o no) de datos de carácter personal de titularidad pública o de titularidad privada, con cierto retraso frente a la legislación estatal europea existente sobre la materia y sobre todo, con los avances tecnológicos del fenómeno TIC e informática [202], que se concretó en la L.O. 5/1992, de

---

(201) En adelante se profundizará sobre el particular y sobre el estudio de la LORTAD, en las partes II, III y IV, por tal motivo, aquí haremos referencia a los comentarios y estudios puntuales que requiere el apartado 4 de ésta parte I, para exaltar la visión iusinformática del derecho a la intimidad y los demás derechos y libertades fundamentales previsto en la CE.

(202) La LORTAD, Ase ha demorado quince años, pero finalmente está ya publicada@, para destacar el epígrafe sobre Ariesgos para los derechos de la personalidad que pueden derivar del acopio y tratamiento de datos por medios informáticos@. Cfr. GONZALEZ NAVARRO Francisco. *DERECHO ADMINISTRATIVO ESPAÑOL*. Ed. Eunsa, 1a., ed. de 1987 y 2a., ed., Pamplona, 1994, pág. 166. En igual sentido, CASTELLS, quien sostiene: ALa aparición de España de una red de tráfico de datos personales obrantes en registros públicos a comienzos de la década de los 90, reveló lo que una política puramente promocional del fenómeno informático, sin suficientes alertas en el plano cautelar, podía ocasionar, *Pérez Luño* ha mencionado A*la paradoja dramática@*, consistente en compensar el retraso en la incorporación al desarrollo tecnológico, con la vanguardia mundial en la piratería del Asoftware@, la delincuencia informática y las agresiones informáticas a la libertad@. Vid. CASTELLS ARTECHE, José M., *DERECHO A LA PRIVACIDAD Y PROCESOS INFORMÁTICOS: ANÁLISIS DE LA LORTAD. R.V.A.P*. Bilbao, 1997, pág. 251.

29 de Octubre conocida como LORTAD. Retraso morigerado, según se ha sostenido porque desde 1984, se conocía Aun conjunto de normas heterogéneas que no siempre distinguían entre ficheros automatizados y ficheros convencionales@ [203] y porque en nuestro criterio, se aplicaba teóricamente la Ley Orgánica núm. 1 de 5 de Mayo de 1982, relativa a la protección civil de los derechos del honor, la intimidad y el propia imagen, como norma jurídica subsidiaria en todos los asuntos relacionados con las intromisiones ilegítimas derivadas del uso de la informática (Disposición Primera Transitoria).

Este antecedente referencial legislativo, condujo a la LORTAD, a decantar y mejorar varias definiciones técnico-jurídicas aplicables al tratamiento informatizado de datos personales y la estructuración de procedimientos técnicos informáticos, a fin de hacerlas más inteligibles al operador jurídico, pero principalmente al juzgador que debe aplicar e interpretar la norma jurídica. Estas definiciones son: a) Datos de carácter personal, b) Fichero automatizado, c) Tratamiento de datos, d) Responsable del fichero, e) Afectado, y f) Procedimiento de disociación (art. 3-a) a f),).

Datos de carácter personal o simplemente datos personales, se considera cualquier información concerniente a personas físicas identificadas o identificables. Esta definición es idéntica a la prevista en el Convenio de 1981, por ello son válidas las observaciones realizadas en aquél aparte. Sin embargo, la LORTAD incluye entre sus definiciones la de Aafectado@, para indicar que se trata de una persona física titular de los datos que sean objeto del tratamiento informatizado, con lo cual abunda sin necesidad sobre el concepto de persona física (identificada o identificable) con el *inri* de que dicha persona no es en *strictu sensu* un *afectado,* sino un interesado, o mejor aún el titular de los datos personales o concernido en un tratamiento o procedimiento informatizado que tiene derechos y también deberes, no simplemente obligaciones o cargas como sugiere el concepto afectado. El titular de datos personales o interesado, contextua la idea de toda

---

(203) El autor cita como ejemplos de dichas normas, entre otras, las siguientes: la LGT (arts. 111 y 112, modif. en 1985 y 1990), la ley 19 /1988 de 12 de julio, de auditoría de cuentas (arts. 13 y 14), y la ley 30/1984, de 2 de agosto, de Medidas para la reforma de la función pública (que prohibía registrar datos Asensibles@ en los expedientes de personal). Refiriéndose ya específicamente a ficheros automatizados cabe citar la legislación electoral y la ley de la Función estadística pública, de 19802. Vid. GONZALEZ NAVARRO, Francisco. *DERECHO... Ob. cit.*, pág. 168.

persona que tiene derechos subjetivos sobre la información relativa a sí misma, aún cuando tal información haya sido reunida por otras personas. Esta visión no sería posible si le anteponemos el calificativo de afectado para referirnos a esa misma persona.

Pero en lo que más destaca la LORTAD, dentro de este aparte de definiciones
es en los conceptos de Atratamiento de datos@ informatizado y de Afichero automatizado@
que el Convenio Europeo de 1981, había definido en forma general y sujeto a interpre-taciones flexibles del operador jurídico con claras deficiencias, tal como se anotó puntualmente, sobre todo respecto al que llamó Atratamiento automatizado@ de datos, excluyendo expresamente el tratamiento no informatizado de datos.

En efecto, la LORTAD, al definir Tratamiento de datos a las *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*, extiende el tratamiento a todo procedimiento técnico no informatizado y estructura el procedimiento de datos personales, a través de un *iter* compuesto de etapas o fases que encadenadas por un tratamiento informático, vale decir, con soportes y medios informáticos, electrónicos o telemáticos se dirigen a producir un dato informatizado, con el cual los responsables de la gestión, los titulares de los datos o los usuarios puedan desarrollar cualquier acción jurídico-técnica posible. v.gr. grabación, almacenamiento, bloqueo o interconexión. La definición de tratamiento de datos, destaca el iter informático que en su conjunto produce un proceso de igual carácter, es decir, un proceso informatizado de datos compuesto de fases o etapas, tales como las iniciales, de desarrollo y terminación. Estas fases, se estructuran con base en los principios fundamentales de la protección de los titulares de los datos personales.

Por su parte, al definir los *Aficheros automatizados@*, como *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, excluye expresamente el concepto de ficheros convencionales, manuales o no informatizados [204], con lo cual se establece una contradicción conceptual con la de tratamiento de datos que incluye a los procedimientos técnicos informatizados y no informatizados . Sin embargo, se ha de interpretar que dicha definición no excluye sino que hace énfasis en el concepto técnico-jurídico de Aautomatizado @ (o, mejor informatizado) y que algunos Ausos@ de los ficheros no informatizados se consideran incluidos, puesto que el ámbito de aplicación de la LORTAD, se extiende a los ficheros automatizados y no automatizados del sector público y privado, siempre que estén registrados en soportes físico compatible de tratamiento automatizado (art. 2).

En las definiciones anteriores se exaltan las etapas o fases del tratamiento informatizado de datos personales que conforman un procedimiento ibídem. En efecto, se destaca las fases de recolección, almacenamiento, registro, conservación y la comunicación (Emisión/transmisión y cesión) de datos personales. En tanto, que las acciones informáticas de revisión, actualización , rectificación, bloqueo y cancelación son originadas tras el ejercicio del derecho de información y acceso que tiene toda persona concernida con datos personales; vale decir, tras el ejercicio del derecho de *habeas data*.

Por ello, Ala Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia@ (E.M. núm. 1).

El *Responsable del fichero*, se considera a la *persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad,*

(204) Ob.ut supra cit., pág. 170

contenido y uso del tratamiento. En esencia, contiene los elementos de la definición inmersos en el concepto de Aautoridad controladora del fichero@, previsto en el Convenio Europeo de 1981, con la diferencia que en éste se especifican las funciones decisorias acerca de cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán a los ficheros, en tanto que la LORTAD, engloba y amplia el radio de acción, al expresar que dichas decisiones se extienden a Alos contenidos y usos del tratamiento@ y no simplemente de los ficheros, en particular.

Efectivamente, como lo sostiene el profesor *González Navarro* **[205]**, aparte de los dos sujetos (titular de los datos y el responsable del fichero), en el tratamiento de datos puede intervenir un tercer sujeto que es Ael contratista o comisionista@ que presta sus servicios de tratamiento informatizado de datos personales dentro de un procedimiento ibídem (art.27). Por su parte, la Ley Federal alemana de protección de datos personales (LFADP) extiende los efectos del principio de responsabilidad en el tratamiento de datos de los denominados Aresponsables del fichero@ a las personas físicas o jurídicas, públicas o privadas que actúan como terceros en el mismo (v.gr. Oficinas de servicios informáticos), tanto de los deberes-derechos que estos tienen, como de las sanciones y la obligación de guardar la confidencialidad de los datos.

De otra parte, se considera *procedimiento de disociación*, a *todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable*. Este derecho-garantía para el titular de los datos personales y el Estado que debe regular, el tratamiento, uso y utilización de los mismos conforme a derecho, tiene aplicación práctica, así: En la distinción de *dato anónimo* **[206]**

(205) Este tercero, según el art. 27 no puede aplicar o utilizar los datos obtenidos con un fin distinto del que figura en el contrato de servicios, ni cederlos a otras personas ni siquiera para su conservación. Igualmente, una vez cumplida la prestación contractual, los datos personales deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se presten tales servicios, porque razonablemente se presumala posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años. Ob. ut supra cit., pág. 170.

(206) Los *datos anónimos*, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general. v.gr. como pueden ser los registros de la propiedad o mercantiles. Por ello, al determinar el ámbito de aplicación de la LORTAD, excluye de la aplicación del tratamiento informatizado de datos personales, los ficheros de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general (art. 2-a).

A*dato reservado*@[**207**], comúnmente empleado en las normas jurídico-penales y iusadministrativistas españolas. En efecto, a pesar de ser ambos datos de carácter personal, pregonables de una persona física, se diferencian en que éste último se predica única y exclusivamente de una persona identificada o identificable, so pena de desvirtuarse, y más aún, no haber existido, si alguna vez eso ocurrió. Tal es el caso, en el ámbito penal y más concretamente al referirse a los delitos contra la intimidad en el título X, Libro II del C.P.Esp., de 1995. Igualmente, en el ámbito administrativo, al referirse a las infracciones al tratamiento informatizado de datos previsto en la LORTAD (arts. 42 y 43).

De igual manera, tiene la aplicabilidad práctica el procedimiento de disociación cuando se refiere a los datos anónimos, a los efectos de hacerles perder la determinabilidad de una persona humana a la que le conciernen los datos de carácter personales. p.e., en los datos estadísticos, históricos, científicos, etc.

4.4.2. PRINCIPIOS FUNDAMENTALES APLICADOS A LAS FASES DEL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES

La institucionalización de Alos principios reguladores de la recogida, registro y uso de datos personales@ (E.M. núm.1) y demás fases o etapas del tratamiento informatizado de datos personales, tales como el almacenamiento, conservación y comunicación constituyen una garantía para el derecho al honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos (art. 1

in fine). Por ello, la existencia de los principios fundamentales del tratamiento informatizado de datos personales sólo encuentra validez, eficacia y presentación en la estructuración de sus

---

(207) De la interpretación doctrinal de los arts. 197.2 y 200 del Código Penal Español de 1995 (en adelante C.P.Esp.), se pueden deducir varios conceptos de dato reservado, a saber: 1. ADato reservado es cual- quier información concerniente a personas físicas identificadas o identificables cuyo conocimiento esta limitado a los usuarios del archivo, registro o fichero automatizado o convencional de acceso restringido. 2. Dato reservado es aquel que es indispensable libremente por terceros, requiriendose para ello autorización de su titular. 3. Dato reservado es aquel que potencialmente puede lesionar el derecho a la intimidad de su titular; en lo que respecta a las personas físicas, y cuyo descubrimiento o revelación debe incidir en la esfera Apersonal o familiar@ de su titular...@ Vid. BAJO FERNANDEZ, Miguel et all. *COMPENDIO DE DERECHO PENAL (Parte Especial).* Vol. II. Ed.Centro de Estudios Ramón Areces, S.A. Madrid, 1998, pág..201-202

fases o etapas, tales como la de recolección, almacenamiento, registro, conservación y comunicación de datos personales, reguladas por la LORTAD e inmersas en dentro del titulo II, sobre principios de la protección de datos: Calidad de los datos (art. 4), Derecho de información en la recogida de datos (art.5), Consentimiento del afectado (art.6), Datos especialmente protegidos (art. 7), Datos relativos a la salud (art.8), Seguridad de datos (art. 9), Deber de secreto (art. 10) y Cesión de Datos (art.11) **[208]**.

4.4.2. 1. FASE INICIAL DE RECOLECCIÓN DE DATOS.

En la *fase inicial de recolección de los datos*, se aplicarán los principios de *la congruencia y racionalidad*, así presentado por la E.M.núm. 1 de la LORTAD, para indicar con ello que sólo se podrán recoger datos personales para su tratamiento automatizado, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se haya obtenido (art.4.1).

Concordantemente con el anterior y por el *principio de calidad de los datos*, se prohíbe la recogida de los datos por medios fraudulentos, desleales o ilícitos (art. 4.7).

Por el principio del *consentimiento, o de autodeterminación* (art. 6), todo tratamiento informatizado de datos, y por su puesto, la recolección de los mismos, Arequerirá el consentimiento@ del titular, interesado o persona concernida, pues con él, se A otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del titular o interesado para que la recogida de datos sea lícita@ (E.M.núm.1).

Sin embargo, no será preciso el consentimiento cuando los datos personales en los siguientes casos: a) Cuando se recojan de fuentes accesibles al público; b) cuando se recojan para el ejercicio de funciones propias de las Administraciones Públicas en el

---

(208) El estudio y análisis de estos principios en las fases o etapas del procedimiento informatizado de datos se profundizará en la parte III y IV., de esta investigación. Por tanto, aquí sólo se referenciarán puntualmente.

ámbito de sus competencias, c) Cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato (art.6-2). Más aún, podrá ser revocado el consentimiento Acuando exista causa justificada para ello y no se le atribuya efectos retroactivos@ (art. 6-3).

Por el *principio de información*, previo al principio del consentimiento y concomitante con el ejercicio de algunos derechos (v.gr. derecho de acceso a la información) y posterior con el ejercicio de otros, tales como el de habeas data, el titular de los datos personales puede informarse plenamente y en forma *a priori*, de qué datos suyos pudieran ser recolectados y sometidos a tratamiento informatizado.

Este principio fundamental que también es un derecho subjetivo de la persona concernida, porque le permite al titular de los datos Aser previamente

informado de modo expreso, preciso e inequívoco@ (art.5-1), cuando sean solicitados datos a él referentes y vayan a ser objeto de recolección y tratamiento informatizado. Quizá, por esto es uno de los principios de importancia capital para el pleno ejercicio del derecho de *habeas data* y los demás derechos y libertades fundamentales, y se aplica no sólo a la fase de recogida de datos sino al conjunto de fases o etapas del tratamiento informatizado de datos, como veremos cuando se interpreta hermenéuticamente el artículo 5 y 13 de la LORTAD. Su operatividad en esta fase, es como sigue:

El titular de los datos personales en la recogida de datos deberá ser informado de modo expreso, preciso e inequívoco [2 09]: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación (*habeas data*); e) De la identidad y dirección del responsable

---

(209) No será necesaria la información a que se refiere el apartado 1 del art. 5 de la LORTAD, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Esto como veremos luego, es objeto de un recurso de inconstitucionalidad ante el TC Español.

del fichero.

4.4.2.2. FASE DE ALMACENAMIENTO DE DATOS.

En la *fase de almacenamiento de datos* se aplicarán los siguientes: a) *El principio de adecuación, pertinencia y no excesibilidad de los datos* con relación al ámbito y las finalidades legítimas (art.1). Este principio que es válido para la recolección de los datos, lo es también para el almacenamiento, por cuanto, éste se requiere para todo dato personal que sea sometido@ a tratamiento@ informatizado, y obviamente el almacenamiento posterior a la recogida de datos es una fase

ineludible del tratamiento; b) El *principio del consentimiento* (art. 6-1), con igual razonamiento al precedente, se aplica este principio a la fase del almacenamiento de los datos, pues el consentimiento del titular se requiere durante todo el tratamiento; c) *El principio de veracidad de la información* (E.M.núm. 1). Los datos personales serán exactos y puestos al día de forma que respondan con veracidad a la situación real del titular (art. 4-3); d) *El principio de información* (arts 12, 4.6 y 13), que opera en todo el tratamiento informatizado de la información y que le permite al titular de los datos ejercer los derechos de acceso, habeas data e impugnación contra actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento o personalidad.

El principio del consentimiento en esta fase del tratamiento es importante, porque Aotorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes@, niveles que Ase refuerzan singularmente en los denominados *´datos sensibles´*, como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece *la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características*. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España@ (E.M.núm. 1).

4.4.2.3. FASE DE REGISTRO DE DATOS.

En *la etapa del Registro de los datos*, se aplica: a) El *principio de exactitud y completud de los datos*. Si los datos personales registrados resultaren ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que los titulares de los mismos devenidas del ejercicio del derecho de *habeas data* -- lla- mados por la LORTAD Aderechos de rectificación y cancelación@ , artículo 15-- (art. 4.4) [2 10]. Así mismo, por aplicación de éste principio, podrán ser cancelados los datos Acuando hayan dejado de ser necesarios o pertinentes para la finalidad para cual hubieren sido recabados o registrados (art. 4.5).

Igualmente se aplicarán los principios del consentimiento, principio de información y el *principio de seguridad de datos*. Este último, como condición *sine cua nom* para el registro de datos, puesto que no se registrarán datos personales en ficheros informatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (art.9-2) [211].

---

(210) *Artículo 15. Derecho de rectificación y cancelación*.1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso. 3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario. 4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos...@ Este artículo ha sido reglamentado por el art. 15 del Dec.1332/1994. En la parte III in fine, puntualizaremos sobre esto.

(211) En la parte III, destinaremos un aparte especial para el estudio de las aplicaciones, soportes y medios informáticos, electrónicos o telemáticos utilizados en el tratamiento informatizado de los datos personales. Legislativamente el Estado Español ha dictado recientemente un Real Decreto núm. 263/1996, de 16 de Febrero, por el cual ARegula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado@, reglamentario del art. 45 de la Ley 30/1992, de 26 de noviembre y aplicable a las Administraciones Públicas Generales del Estado.

Por *el principio de la confidencialidad de los datos*, aplicable a todo el tratamiento informatizado de datos, pero particularmente a las fases de registro, conservación y comunicación de datos, el responsable del fichero y quienes intervengan en Acualquier fase del tratamiento de los datos@ personales están

obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo (art. 10).

4.4.2.4. FASE DE CONSERVACION DE DATOS.

En esta fase del tratamiento informatizado se aplicará: a) El *principio de la tem-poralidad de los datos*. Aplicable en dos formas: 1. no se serán conservados en forma que permita la identificación del titular de los datos durante un período superior al necesario para los fines en base a los cuales hubieran, salvo que deban mantenerse en su integridad atendiendo al valor histórico que los datos puedan tener de conformidad con el ordenamiento jurídico vigente. (art. 4.5 *in fine*); y 2. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el titular de los mismos (art.15.5).

b) Por el *principio de seguridad de los datos,* el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (art. 9-1).

c) Por *el principio de tutela de derechos del titular de los datos*, integrado por los anteriores principios y los referentes al derecho de *habeas data,* el titular podrá ejercer el derecho de acceso, a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes --art. 14-3-- [212].

Igualmente son aplicables los principios del consentimiento y principio de información, los cuales son deben observarse en todo procedimiento o tratamiento informatizado de datos.

4.4.2.5. FASE DE COMUNICACION DE LOS DATOS.

Esta fase del tratamiento informatizado se estructura en la emisión y transmisión de los datos personales, a través de soportes y medios informáticos, electrónicos o telemáticos idóneos para la comunicación o la cesión de los mismos. Se entiende por *cesión de datos*, toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero; y sobre todo, la actividad de interconexión con otros ficheros y la comunicación de los datos realizada por una persona distinta del titular de los datos personales.

En consecuencia, serán aplicables los principios de consentimiento, información, confidencialidad y seguridad de los datos, por tener aplicabilidad en todas las fases del tratamiento informatizado.

Por *el principio del consentimiento o autodeterminación* del titular de los datos, la LORTAD,

> Ase propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completa el principio del consentimiento, exigiendo que, al procederse la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona (art. 8.2) y del Convenio 108 del Consejo de Europa (art. 9.2), que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla.@ (E.M. núm. 2)

---

(212) *LORTAD. Art. 14. Derecho de acceso*.@1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados. 2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de

los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos@.

La regla general establecida en la LORTAD referente a la cesión de datos, es que con objeto del tratamiento informatizado de datos personales sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del titular de los datos (art.11-1). El consentimiento debe reunir los requisitos de forma y de fondo establecido en la LORTAD para que tenga aplicabilidad en la fase de cesión, de lo contrario podrá ser anulado, revocado o incluso no requerido, si previamente se aplicado procedimiento de disociación a los datos [213].

Sin embargo, como excepciones a la regla se establecen los siguientes casos: a) Cuando una Ley prevea otra cosa; b) Cuando se trate de datos recogidos de fuentes accesibles al público; c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique; d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas; e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos de diversidad de competencias y creación de ficheros; y , f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero informatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad (art. 11-2).

El *principio de libre circulación de datos,* aplicable a las comunicaciones de datos personales denominado por la LORTAD, como Amovimiento internacional de datos@ (art. 32). En este punto, la Ley traspone la norma del artículo 12 del

Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo

---

(213) Art. 11-3, LORTAD,. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente. 4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable. 5. El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la LORTAD. 6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con *el libre flujo de los datos*, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias. (E.M. núm. 4 *in fine)*

4.4.3. ORGANOS DE PROTECCIÓN DE LOS DATOS PERSONALES.

La LORTAD establece como órganos de la protección de los datos personales a los siguientes: a) La Agencia de protección de datos, que como organismos de régimen jurídico *sui géneris* cuenta con un Director asesorado con un AConsejo Consultivo@; b) El Registro de protección de datos, como órgano integrado a la Agencia; la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia (art. 11-3,

R.D.núm.428/1993, de 26 de Marzo).; y c) Organos de protección de datos de las Comunidades autónomas [214].

4.4.3.1. LA AGENCIA DE PROTECCIÓN DE DATOS.

La Agencia de Protección de Datos Española, es la entidad pública, con perso-

---

(214) A efectos prioritarios de la investigación nos referiremos a la Agencia y el Director de Protección de Datos, pues los otros organismos han sido puntualmente tratados por Francisco González Navarro, José María Souvirón, Fairen Guillen, Castells Arteche, en sus diferentes obras ut supra citadas. Sin embargo, destaque-mos que *el Consejo Consultivo* que asesora al Director de la Agencia, es Aun órgano de apoyo definido por los caracteres de colegiación y representatividad, en el que obtendrán presencia las Cámaras que representan a la soberanía nacional, las Administraciones Públicas en cuanto titulares de ficheros objeto de la presente Ley, el sector privado, las organizaciones de usuarios y consumidores y otras personas relacionadas con las diversas funciones que cumplen los archivos informatizados@ (M.E.núm 5).

nalidad jurídica propia y plena capacidad pública [215] y privada [216], que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones, con un régimen jurídico *sui géneris* (integrado por la LORTAD, un Estatuto propio dictado por el Gobierno R.D.núm.428/1993, de 26 de Marzo [217]; así como, la disposición tipo Acajón de sastre@ [218] del art.6.5. LGP). La Agencia, tiene como objetivo prioritario velar por el cumplimiento de la legislación en materia de protección de datos personales informatizados en España, pero particularmente, la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de octubre, de *Regulación del Tratamiento Automatizado de los Datos de Carácter Personal* y los derechos y libertades fundamentales e intereses legítimos implicados en ella.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un numerus clausus de causas de cese

---

(215) En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la LORTAD y sus normas de desarrollo (El Real Decreto 428/1993, de 26 de Marzo, reglamentario de la LORTAD, conocido

como Estatuto de la Agencia de Protección de Datos)., la Agencia actuará de conformidad con la ley de Pro-cedimiento Administrativo (antes LPA.; hoy, LRJAP: Ley de Régimen Jurídico de las Administraciones Públicas y procedimiento administrativo común. Ley 30/1992, de 26 de Noviembre)-- Art. 34.3 LORTAD--. Vale decir, que a este tipo de funciones se aplica un régimen jurídico de derecho público, donde la LORTAD es la norma especial y la LRJAP, es la norma subsidiaria para llenar lagunas y vacíos normativos de aquélla.

(216) En su adquisiciones patrimoniales y contratación estará sujeta al Derecho privado. Este dual régimen jurídico (público y privado) aplicable por la Agencia de Protección de datos es lo que caracteriza un régimen sui géneris, además de la condición de entidad (por AEnte@) de derecho público con funciones públicas y privadas a la vez e independiente de las Administraciones Públicas.

(217) El R.D.núm. 428 /1993, lo concreta normativamenta así: AArtículo 2. *Régimen jurídico*.1. La Agencia de Protección de Datos goza de personalidad jurídica propia y plena capacidad pública y privada. 2. La Agencia de Protección de Datos se regirá por las disposiciones legales y reglamentarias siguientes: a) El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. b) El presente Estatuto y las demás disposiciones de desarrollo de la Ley Orgánica 5/1992. c) En defecto de las anteriores, y para el ejercicio de sus funciones públicas, las normas de procedimiento contenidas en la Ley 30/1992, de 26 de noviembre, ARégimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común@. d) Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación. e) Cuantas otras disposiciones resulten de aplicación. 3. La Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia. 4. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

(218) Así lo califica el profesor *González N.*, al Aart. 6.5 de LGP --Ley General de Presupuesto, del cual dice-- quedará en la historia de derecho público como ejemplo de lo arriesgado que resulta al poner en manos de los adoradores del Poder preceptos tipo Acajón de sastre@. Con base esa norma se van aumentando los organismos autónomos o independientes que buscan el camino de la Alibertad@ (entiéndase: de la reducción al máximo de cualquier forma de control). GONZALEZ NAVARRO, Francisco. *COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y EL PROCEDIMIENTO ADMINISTRATIVO COMUN.*, 1a., ed., Ed. Civitas S.A., Madrid, 1997, pág.705.

La Agencia de Protección de datos tendrá como funciones, las siguientes:

1. *Funciones de control y vigilancia*:

La Agencia de Protección de datos tendrá como funciones el velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos. Así mismo:

a) Ejercerá el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen (SIS) (art. 10 R.D.428/1993), b) Velará por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicará y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información adicional que determine el

Director (LORTAD, art. 36-j., art.7 R.D.428/1993), c) ejercerá el control de la observancia de lo dispuesto en los artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial: i) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadísticos. ii) Dictaminará sobre los procesos de recogida y tratamiento automatizado de los datos personales a efectos estadísticos. iii) Informará sobre los proyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley de la Función Estadística Pública. iv) Dictaminará sobra las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos (art. 7 R.D.428/1993).

Igualmente, tendrá como funciones de control y vigilancia: a) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias (art.36-b LO 5/1992), b) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LORTAD (art. 36-c LO 5/1992), c) Atender las peticiones y reclamaciones formuladas por las personas afectadas (art. 36-d, LO 5/1992), d) Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la presente Ley (art. 36-f, LO 5/1992) y, e) Ejercer la potestad sancionadora en los términos previstos por el título VII de la LORTAD, (art.36-g. LO 5/1992, o Aproceso descodificador@(por *decodificador*) establecido por la LRJPA [219].

2. *Funciones de Relaciones con los titulares de los datos*:

a) La Agencia informará a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social (art. 4-1 R.D.428/1993) y, b) La Agencia atenderá las peticiones que le dirijan los afectados y resolverá las reclamaciones formuladas

por los mismos, sin perjuicio de las vías de recurso procedentes (art. 4-2. R.D.428/1993).

3. *Funciones de Cooperación y Asistencia entre organismos*:

a) La Agencia cooperará con los organismos internacionales y órganos de las Comunidades Europeas en materia de protección de datos (art 9-1.R.D.428/1993), b) prestará asistencia a las autoridades designadas por los Estados parte en el Convenio Europeo de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos de garantizar el derecho de información de los titulares de los datos en dicho tratamiento (art 9-2. R.D.428/1993) y, c) colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la LORTAD (art.5 R.D.428/1993)

4. *Funciones de presentación de Memorias e informes*:

a) La Agencia de Protección de Datos redactará una Memoria anual, la cual será

---

(219) Ibídem., pág. 706.

remitida por el Director al Ministro de Justicia, para su ulterior envío a las Cortes Gene- rales, sobre la aplicación de la LORTAD y demás normas reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre el funcionamiento de la Agencia: i) Una relación de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos, ii) Un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos. 3. Un análisis y una valoración de los problemas de la protección de datos a escala nacional (art. 6. R.D.428/1993) y, iii) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal (art.36-e, LO.5/1992); c) Informar,

con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley (art. 36-h. LO 5/1992); y, d) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones (art.36-i, LO 5/1992).

5. *Funciones de Inspección*:

La Agencia de Protección de datos podrá Inspeccionar los ficheros tanto de titularidad público como de titularidad privada, recabando cuantas informaciones precise para el cumplimiento de sus cometidos. A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior, tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Así mismo, estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas (art.39 LO 5/1992).

4.4.3.2. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS.

El *Director de la Agencia de Protección de Datos,* dirige la Agencia y ostenta su representación. Prioritariamente el Director hará cumplir y cumplirá todo lo atinente a la legislación sobre tratamiento informatizado de datos personales y en su carácter de funcionario ejecutor de las políticas, recomendaciones y sugerencias de la Agencia de Protección de Datos, velará y controlará el ejercicio de los derechos de información, *habeas data* (acceso, actualización, rectificación , bloqueo y cancelación de datos) y el pleno de derechos y libertades fundamentales e intereses legítimos.

El Director será nombrado, de entre quienes componen el consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Cesará antes de la expiración del período, por las siguientes causas: 1. A petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo; 2. Por incumplimiento grave de sus obligaciones, 3. Por incapacidad sobrevenida para el ejercicio de su función, y, 4. por incompatibilidad o condena por delito doloso.

El Director de la Agencia, tiene una gama variopinta de funciones, tales como las de Dirección [220], de Gestión [221] y designación [222], que apuntan a determinar que su cargo se desempeña con dedicación absoluta, plena independencia y total objetividad, y por ello no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna (art. 16 R.D.428/1993). Gozará de los mismos honores y tratamiento que los subsecretarios del Estado (art. 14-2 Ibídem).

---

(220) A título de ejemplo: ADictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial: a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos. b) Requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo. c) Resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados. d) Autorizar transferencias temporales o definitivas de datos que hayan sido objeto de tratamiento automatizado o recogidos a tal efecto, con destino a países cuya legislación no ofrezca un nivel de protección equiparable al de la Ley Orgánica 5/1992 y el presente estatuto...@ (Art. 12 R.D.428/1993).

(221) A título de ejemplo: a) Adjudicar y formalizar los contratos que requiera la gestión de la Agencia y vigilar su cumplimiento y ejecución. b) Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia (art. 13 Ibídem).

(222) Designará a dos (2) representantes para la autoridad de control común de protección de datos del Sistema de Información Schengen (art.10-2, R.D.núm.428/1993).

4.4.4. INCONSTITUCIONALIDADES DE LA LORTAD, QUE AFECTAN EL TRATAMIENTO Y PROCESO INFORMATIZADO DE DATOS.

Existen actualmente varios recursos de inconstitucionalidad en contra de la LORTAD (L.O. 5/1992, Oct. 29), los cuales han sido presentados por el Defensor del Pueblo [223], El Parlamento Catalán [224], El Consejo Consultivo de la Generalidad

---

(223) EL DEFENSOR DEL PUEBLO interpuso el núm. 219/1993 contra el art. 19-1 de la LORTAD [@Cesión de datos entre Administraciones Públicas. 1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de sus competencias, *salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso@*]; y el art.22-1 de la LORTAD [Otras excepciones a los derechos de los afectados. 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de *las funciones de control y verificación de las Administraciones Públicas* de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o *a la persecusión de infracciones* penales o *administrativas@* y el art. 22-2 Ibídem [2. *Lo dispuesto en el art. 14 y en el art. 1 del artículo 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección.* Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas@]. Las partes en cursiva son las cuestionadas constitucionalmente. Argumento principal: Quebrantamiento del principio de reserva de ley (art. 53.1 CE). Anotaciones referenciales sobre la materia, en: CASTELLS ARTECHE, José M. *DERECHO A LA PRIVACIDAD Y PROCESOS INFORMATICOS: ANALISIS DE LA LORTAD*. R.V.A.P. Bilbao, 1997, pág. 253

(224) EL PARLAMENTO DE CATALUÑA EN 1993, propuso recurso de inconstitucionalidad contra los arts. 24 LORTAD [Artículo 24. Notificación e inscripción registral. 1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar. 3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero automatizado si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos]; Art. 31 LORTAD [Artículo 31. Códigos tipo. 1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas]; Art. 40.1 Ibídem [Artículo 40. Organos correspondientes de las Comunidades Autónomas. 1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido]; y Art. 40.2. Ibídem [2. Las

de Cataluña [225] y el Partido Popular [226], ante el Tribunal Constitucional Español que aún permanecen irresolutos y que inciden sobre la columna vertebral del tratamiento y proceso informatizado de datos personales y la distribución competencial en estas materias entre el Estado y las Comunidades Autónomas, con lo cual se transgrede el llamado ABloque de Constitucionalidad@ previsto en el Ordenamiento Jurídico Español. Sin embargo, a los efectos de esta investigación nos detendremos en el análisis de los recursos de inconstitucionalidad a los artículos de la LORTAD que vulneran los *principios y derechos fundamentales* de los titulares de los datos personales en el tratamiento y proceso informatizado, pues estos, como apunta el profesor *Morales Prats* [227], tienden a *rebajar incluso los mínimos de tutela que marca el Convenio Europeo de 1981 en la informatización y manejo de los datos personales en el ciclo operativo de los bancos de datos*.

Sea lo primero, decir que muchos de los recursos de inconstitucionalidad que hoy permanecen *sub judice* ante el Tribunal Constitucional, se ven tocados en su esencia

---

---Continuación nota 224--

Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos]. Argumento básico: Desconocer el marco de distribución competencial entre el Estado y las Comunidades autónomas infringiendo así el llamado bloque de constitucionalidad. Distribución competencial que no abarca la competencia exclusiva del Estado en materia de derechos y libertades fundamentales, previstos en el art. 149.1 CE.

(225) EL CONSEJO EJECUTIVO DE LA GENERALIDAD DE CATALUÑA interpuso recurso de inconstitucionalidad contra los arts. 24, 31, 39, 40.1 y 2, y la disposición final tercera de la LORTAD [Tercera. Preceptos con carácter de Ley ordinaria. Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley ordinaria]. Los Recursos del Parlamento y Consejo Consultivo de la Generalidad Catalana, como sostiene *Souvirón*, están basados en un dictamen del Consejo Consultivo de la Generalidad, de 23 de diciembre de 1992, según el cual resultarían inconstitucionales los arts. 5.2, 19.1, 20.3, 21.1, 22, 24, 31 y 40.1 y 2 LORTAD, reivindican la competencia de las Comunidades Autónomas sobre los ficheros de titularidad privada y los de la Administración Local que la LORTAD atribuye a la Administración del Estado@. Vid. SOUVIRON, José María. *EN TORNO A LA JURIDIFICACION DEL PODER.... Ob. cit.*,pág. 142.

(226) EL GRUPO POPULAR interpuso recurso de inconstitucionalidad contra los artículos 6.2 [Artículo 6. Consentimiento del afectado. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato] y los arts. 19.1, 20.3 [Artículo 20. Ficheros de las Fuerzas y Cuerpos de Seguridad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de

Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.], arts. 22.1 y 22.2 Ay los demás que procedieren por conexión@

(227) MORALES PRATS, Fermín. COMENTARIOS A LA PARTE ESPECIAL DEL CODIGO PENAL. En: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio. Ed. Aranzadi, Pamplona (Nav.), 1996, págs.309 y ss..

antes y después de expedida y puesta en vigor la LORTAD, por normas comunitarias europeas que regulan el tratamiento informatizado de los datos personales y la protección de las personas físicas en el pleno ejercicio de los derechos y libertades fundamentales e intereses legítimos con relación a aquél.

En efecto; la primera, es el Convenio del Consejo de Europeo de 1981, ratificado por España, mediante Instrumento de 24 de Enero de 1984, el cual forma parte del Ordenamiento jurídico interno español (art.96.1 CE. Publicado en el BOE, Nov.15/1985); y además, constituye un instrumento jurídico con alcance interpretativo de los derechos y libertades fundamentales reconocidos por la CE (art. 10.2) , y particularmente de los derechos al honor, a la intimidad personal y familiar Ay el pleno ejercicio de sus derechos@ --art.18.4 CE-- (STC 254/1993, de 20 de Julio. BOE del 18 de Agosto), cuando se aplica al tratamiento informatizado de datos personales, ante la ausencia legislativa de una norma jurídica en vigor en España que regulara dicho tratamiento en la fecha de ocurrencia de los hechos y de presentación de la demanda ante los Tribunales Contencioso-administrativos e incluso de la fecha de presentación del recurso de amparo ante el Tribunal Constitucional de España [228].

La segunda, consistente en la transposición de la normativa comunitaria al ordenamiento jurídico español, básicamente de dos Directivas Comunitarias que aluden al tratamiento informatizado de datos personales y su incidencia con los derechos y libertades fundamentales reconocidos en la CE. Estas son: a) la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y, b) la Directiva 97/66/CE, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y _____

(228) Los hechos del que se ha conocido en la doctrina española como el ACaso Olaverri@, se inician por la pe- tición del Sr. Francisco Javier, en febrero de 1986, dirigida al Gobernador Civil de Guipuzcua con miras a proteger sus derechos fundamentales de la intimidad y la imagen (F.J.2 STC.254/1993). Petición que se concretaba en solicitar al Gobierno Civil si existían o no datos de carácter personal que le conciernan en el fichero informatizado que la Administración del Estado manejaba o gestionaba. Los Tribunales Contencioso-administrativos , desestimaron los recursos de D. Francisco Javier, básicamente porque Ael Convenio (Europeo de 1981) no era de aplicación directa, siendo preciso el complemento de la actividad legislativa y reglamentaria interna para la aplicación práctica de sus disposiciones en España@ (F.J.1 Ibídem), lo cual obligó al petente a recurrir ante el Tribunal Constitucional en recurso de amparo de sus derechos fundamentales.

las redes móviles digitales públicas. Transposición normativa que el caso del derecho español, deberá haberse verificado el 28 de Octubre de 1998, al menos para la Directiva 95/46/CE, tal y como lo prevé aquélla en las disposiciones finales (art. 32) [229] .

En consecuencia, atendiendo a la estructura de estudio y análisis que venimos haciendo de las normas estatales y comunitarias que regulan el tratamiento y proceso informatizado de datos personales, haremos mención a los recursos de inconstitucionalidad a los artículos de la LORTAD que afectan a los principios de información y los componentes del derecho de *habeas data* (acceso, actualización, rectificación, bloque y cancelación de datos); el principio del consentimiento en las fases o etapas de recolección, de almacenamiento, de registro y comunicación (prioritariamente en la Acesión de datos@) de datos personales; y, el principio de reserva de ley para el ejercicio, garantía y protección de derechos y libertades fundamentales (art.53-1 CE). Principios fundamentales obviamente contenidos en derechos de igual rango que se ven vulnerados por la actual regulación de la LORTAD, aunque hay quienes sostienen [230], que la inconstitucionalidad de la LORTAD, no se debe a *una escasa o deficiente regulación de los derechos del ciudadano o de las garantías reconocidas para el pleno ejercicio de los mismos, sino de las múltiples excepciones que dentro de dicho texto se prevén para unos y otras.* Sin embargo, son de tanta envergadura las excepciones que vacían de contenido, o más aún desvirtúan la esencia o núcleo del derecho que las contiene.

4.4.4. 1. PRINCIPIO FUNDAMENTAL DE LA INFORMACION Y EL *HABEAS DATA*.

(229) La Directiva 95/46/CE. AConsiderando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste-eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento@ (Considerando 69). Texto en WWW.CC.CEC(Database CELEX).

(230) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, Antonio. *SOBRE LA INCONSTITUCIONALI- DAD DE LA LEY DE PROTECCION DE DATOS INFORMATICOS.* En: Revista Actualidad Aranzadi. Núm. 8 de Julio, Pamplona, 1993, pág. 6.

Inaplicación del derecho a la información y el ejercicio del *habeas data (art.5*.3, en relación con el art. 5-1).

Se ha sostenido, que el derecho a la información y el derecho de *habeas data* aplicables al tratamiento informatizado de datos y previstos en la LORTAD (arts. 5 y 13 y 14 a 16, respectivamente) con carácter *in genere* a la totalidad de las fases o etapas del ciclo informático de las bases de datos personales, constituyen además principios fundamentales de expresa observancia por quienes están involucrados en estos procesos de características técnico-jurídicas especiales, tal y como son, los informatizados de datos personales.

El principio-derecho a la información que tienen los titulares de los datos constituye una garantía *a priori y* concomitante a un tratamiento informatizado de datos por quienes estén involucrados en dicho proceso (especialmente los responsables de los ficheros y/o autoridades competentes en dicho proceso), pero particularmente en la fase inicial de recolección de los datos personales, deberán previamente informar de modo expreso, preciso o inequívoco, a los interesados, acerca: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, c) De las consecuencias de la obtención de los datos o de la negativa a

suministrarlos, d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación y, e) De la identidad y dirección del responsable del fichero (Art.5-1).

Sin embargo, se cuestiona la constitucionalidad del art.5-3, que prevé excepciones a la regla general del art.5-1, cuando expresa: A*No será necesaria la información a que se refiere el apartado 1, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban*@.

Estas excepciones al derecho de la información y el ejercicio de los derechos de *habeas data* (acceso, rectificación y cancelación), plasmados en la norma recurrida ante el Tribunal Constitucional Español, desvirtúa y vacía de contenido la regla general, basado en una cláusula general indeterminada, asentada en criterios vagos (*la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban* [231]) y utilizada para recortar arbitrariamente uno de los derechos esenciales del ´*habeas data*´ del ciudadano, reconocido en el art. 18.4 [232], en Acuanto que habría un grave peligro para la intimidad ... (y el pleno ejercicio de los derechos del ciudadano previstos en la CE, con lo cual también se vulnera) el artículo 9.3 de la Constitución, que garantiza la *seguridad jurídica* [233].

Igualmente se endilga razones de inconstitucionalidad al art. 5-3, no sólo por rebajar el mínimo de garantías denominadas Acomplementarias para la persona concernida@, prevista en el art. 8 Convenio Europeo de 1981, de parecida redacción al art.5.1 LORTAD (aunque mucho más recortado que el del Convenio, lo cual *per se* ya es un motivo de desconocimiento del Amínimo irreductible@ de derechos del titular), sino por desconocer flagrantemente el marco de las causales *numerus clausus*, que como excepciones taxativas se plantean a los derechos de información y al ejercicio del derecho de habeas data en el art. 9 del Convenio Europeo de 1981., y consistentes en la Seguridad del Estado, la Seguridad Pública, los intereses monetarios del Estado o la represión de infracciones penales, así como la protección de la persona concernida y los derechos y libertades de otras personas. Incluyo se

desconoce el marco de las que el Convenio de 1981, denomina Arestricciones@ (que jurídica y strictu sensu no son Aexcepciones@) a los derechos de información y de habeas data (que abarca además a los derechos de borrado o de recurso, si fuere el caso), para Alos ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas@ (art. 9-3).

---

(231) Según, *López G.*, AEstos términos conceden al funcionario o empleado encargado de suministrar los datos, un ámbito de discrecionalidad tan amplio que se confunde con la arbitrariedad y que hace perder todo senti- do a las garantías establecidas en el apartado 1 del art. 5". LOPEZ GARRIDO, Diego. *ASPECTOS DE INCONSTITUCIONALIDAD DE LA LEY ORGANICA 5/1992, DE 29 DE OCTUBRE*. En: Revista de Derecho Político. Universidad nacional de Educación a Distancia, UNED. Núm. 38, Madrid, 1993, pág. 24.

(232) MORALES PRATS, Fermín. COMENTARIOS A LA PARTE... Ob.cit., pág.309 y ss.

(233) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 24.

Excepciones a los derechos de los titulares de los datos en los Ficheros de Titularidad pública (art. 22.1., en relación con el art. 5-1 y 5-2; y, art. 22.2, en relación con los arts. 14 y 15-1).

Por su parte, se considera inconstitucional el art. 22.1 de la LORTAD, que inaplica el art. 5-1 y 2 de la misma Ley Orgánica, contentivos de los derechos a la información y de habeas data que tiene el titular de los mismos, en la fase o etapa inicial de recolección de datos personales informatizados e incluso no informatizados (al hacer mención Acuestionarios u otros impresos para la recogida de datos@), según dice el art. 22.1, A cuando la información al titular impide o dificulte gravemente el cumplimiento de las *funciones de control y verificación de las Administraciones Públicas* o cuando afecte a la Defensa Nacional, a la seguridad Pública o a la persecución penales o *administrativas@.*

Esta inaplicación legislativa del derecho a la información, que no es una excepción jurídicamente hablando, sino una abrogación normativa del propio legislador y que en la doctrina ibérica se ha entendido como una Adenegatoria@ de aquél derecho, basados en causales indeterminadas, abstractas y vaporosas, como son el impedimento o dificultad grave del cumplimiento de funciones

gubernamentales. Aunque se expresa que dichas funciones son las Acontrol y verificación de las administraciones Públicas@, estas son tan amplias como indeterminadas, máxime cuando un grupo amplísimo de las funciones gubernamentales tienen por objeto las actividades controladoras o verificadoras de actos, hechos, acciones o omisiones tanto subjetivas como objetivas de los ciudadanos, de los funcionarios y la propia Administración. La Administración en este caso carece de límites claros y precisos que le obliguen a dar prevalencia al derecho que tiene el ciudadano a ser informado de las garantías en la recogida de datos, lo que sería incompatible con el principio de seguridad jurídica y de interdicción de la arbitrariedad (art.9.3 CE), o incluso contrario al art. 10.2 y 53.1, ya que esas excepciones no respetan el contenido esencial ni una adecuada interpretación conforme al Convenio de 1981, del derecho a la intimidad personal y familiar y el pleno ejercicio de los demás derechos previstos en la CE [234].

---

(234) QUILEZ AGREDA, Ernesto y otro. Ob. ut supra cit., pág. 7.

Igualmente se reputa como inconstitucional, el art.22.1, porque la mencionada inaplicación legislativa, se extienda a causales que incluso desbordan el régimen de excepciones y restricciones previsto en el Convenio Europeo de 1981, cuando deja de aplicar el art. 5-1 y 5-2, a Ala persecución... administrativas@, causal ésta que junto a las anteriores, se prevén en el art.9, como Aexcepciones a las garantías de@ aquél, según lo sostiene *López Garido*, se vulnera así, el Acontenido esencial de los derechos protegidos en el art.18.4 CE@ (STC 11/1981, de 8 de abril [235]).

Con mayor incidencia, el art. 22.2 LORTAD, se reputa inconstitucional, porque éste inaplica lo dispuesto en el art. 14 y 15-1, es decir, que desconoce el ejercicio de los derechos estructurales del derecho de *habeas data* (acceso, rectificación y cancelación), que esta garantizado por la CE, como por el Consejo de Europa de 1981, para todo ciudadano o titular de los datos personales. La inaplicación del derecho de *habeas data*, opera, según la norma cuestionada por

inconstitucionalidad, Asi ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado (por interesado) hubieran de ceder ante razones de *interés público* o ante *intereses de terceros* más dignos de protección@.

La inaplicación legislativa al ejercicio del derecho de habeas data, Aconstituye una cláusula indeterminada que posibilita la arbitrariedad frente al ejercicio del *habeas data*, y debe reputarse vulneradora de lo dispuesto en el art.9 del Convenio del Consejo de Europa y, por ende, del art. 18.4 CE@ [236].

Igualmente, es inconstitucional la norma jurídica en la utilización de términos

---

(235) Citada por López Garrido, la cual expresa: AConstituyen el contenido esencial de un derecho subjetivo aquellas facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a este tipo y tiene que pasar a quedar com- prendido en otro desnaturalizándose.... Se puede entonces hablar de una esencialidad del contenido del derecho para hacer referencia a aquella parte del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección... Se entiende por contenido esencial aquella parte del contenido de un derecho sin la cual éste pierde su peculiaridad, o dicho de otro modo, lo que hace que sea recognoscible como derecho perteneciente a un determinado tipo. Es también aquella parte del contenido que es ineludiblemente necesaria para que el derecho permita a su titular la satisfacción de aquellos intereses para cuya persecusión el derecho se otorga@. LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 18

(236) MORALES PRATS, F. Ob. cit., pág.309 y ss.

Aintereses de terceros@, por ser excesivamente amplios e indeterminados y rebasar las excepciones previstas en el art. 9 del Convenio Europeo que justifica la excepción a las garantías establecidas cuando se tomen medidas necesarias en una sociedad democrática para la *protección de la persona concernida y de los derechos y libertades de otras personas*. Parece claro, como sostiene *López Garrido* [237], que los términos Aderechos y libertades@ son mucho más concretos y específicos que los términos Aintereses@ que emplea el art. 22.2. Más aún, son términos difusos y abstractos.

4.4.4. 2. PRINCIPIO FUNDAMENTAL DEL CONSENTIMIENTO Y EL *HABEAS DATA*.

1. Tratamiento informatizado de datos personales considerados sensibles, aún con el consentimiento --expreso y escrito o meramente manifestado-- (Art.7 en relación con el art. 6.1) .

La expresión exterior del consentimiento humano (en forma escrita o tácita), constituye el basamento de todo proceso informatizado de datos personales (generales o Asensibles@) en el ordenamiento jurídico ibérico sobre la materia. Por ello, se ha elevado a rango de principio fundamental en la LORTAD, principio del consentimiento que rige para todo tratamiento informatizado y en todas sus fases (recolección, almacenamiento, registro, conservación y comunicación) constitutivas de proceso ibídem, aunque a veces, la propia ley acentúa su énfasis de protección a alguna de las fases por el acrecentamiento del riesgo o vulnerabilidad que aquellas representan frente a las acciones que pretenden desvirtuarlas tras el desconocimiento de derechos y libertades fundamentales, tanto por particulares como por personas físicas o jurídicas de derecho público. v.gr. En el almacenamiento de datos sensibles (art. 4-2): El caso de la huelga en la ARENFE@ (Ferrocarriles de España) y la nómina del personal [238].

---

(237) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 31-33.

(238) Vid. Sentencia del Tribunal Constitucional (TC), 11/1998, de 13 de enero. La empresa estatal RENFE, en el mes de mayo de 1994, retiene una cantidad del salario de un trabajador de la empresa, por la su- puesta participación en los paros de los meses anteriores. Retención que se hace de la nómina informa- tizada (base de datos) que gestiona la empresa. El trabajador agota todas las instancias jurisdiccionales hasta incoar el Recurso de Amparo ante el TC. Ante el TC, considera que se le han vulnerado la libertad sindical (art. 28 CE), en conexión con los arts. 16.1, 18.1 y 18.4 CE, así como los artículos 4.2 y 7.1, LORTAD. El TC, en su fallo analiza los planteamientos, y sobre todo en lo que aquí nos interesa, los quebrantamientos del art. 18.4 CE y los artículos de la LORTAD, con base en los planteamientos vertidos en otro caso y fallo ilustre sobre la materia: la Sent. 254/1993, para concluir que efectivamente dichos textos normativos se han visto vulnerados por la actuación de la empresa recurrida. Un análisis más detallado de esta sentencia se hace en el punto 3 de la parte I., de esta investigación.

Por su parte, el art. 6 del Convenio Europeo de 1981, proscribe todo proceso informatizado de datos personales considerados sensibles (relativos a la vida sexual, el origen racial, la salud, las creencias, la ideología, las opiniones políticas, las convicciones religiosas u otras convicciones), a menos que el derecho interno prevea

garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal
referentes a condenas penales.

Pues bien, la LORTAD en el art. 6 y 7, al permitir el tratamiento informatizado de datos personales sensibles, aún con ciertas garantías que se consideran insuficientes a la vista de las normas universales, y en especial del Convenio de 1981, se estima que no se halla dentro de ese margen exceptivo de Agarantías apropiadas@ exigido por el art.6 *in fine* del Convenio de 1981, por el sólo hecho de exigir el consentimiento expreso y escrito para ciertos datos sensibles (ideología, religión y creencias) o el mero consentimiento para otros (datos que revelen origen racial, salud y la vida sexual), o establecer una especie de *cautela* [239] de protección para algunos datos sensibles (ideología, religión, creencias, origen racial o vida sexual. Art. 7-4), por la cual se prohíbe crear ficheros Acon finalidad exclusiva de almacenar datos@, haciendo énfasis solamente a la fase de almacenamiento de datos personales, como si fuera la única etapa de alto riesgo o vulnerabilidad en un proceso informatizado de datos.

Más aún, como sostiene el profesor *Morales Prats* [240], la LORTAD no ofrece un régimen de garantías suficientemente firme para la informatización de los referidos datos. Así, para los datos relativos a la ideología se limita a exigir el consentimiento del titular de los datos por escrito; con respecto a los datos relativos al origen racial o a la vida sexual, el art. 7 LORTAD se limita a exigir que concurran razones de Ainterés general@ reconocidas por una ley, que justifiquen la informatización, lo cual contraria el art. 6 del Convenio de 1981, pues no se encuentran razones que justifiquen la informatización de los datos personales sobre la vida sexual o el origen racial del individuo. La informatización de estos datos sólo puede albergar un interés

---

(239) MORALES PRATS, F. Ob. cit., pág.309 y ss.
(240) Ibídem, pág. 309 y ss.

legítimo de tipo estadístico y, para tal menester, no es precisa la identificación del titular de los datos; por tanto, la LORTAD debía haber exigido como garantía la previa disociación de éstos, al objeto de que el titular no pudiera ser identificado.

B. Excepciones al derecho de acceso, rectificación y cancelación en los Ficheros de Titularidad Pública, sin el consentimiento del titular de los datos (art.21, en relación con los arts. 7-2 y 7-3).

El artículo 21 de la LORTAD, es severamente cuestionado en su constitucionalidad por desconocer flagrantemente los derechos estructurales del ejercicio del derecho de *habeas data y el principio del consentimiento* que todo titular de los datos personales ostenta en el tratamiento o proceso informatizado de datos en el Ordenamiento Jurídico Español, sobre la materia.

En efecto, el art. 21 LORTAD, inaplica la normativa prevista en el artículo 7.2 y 7.3 LORTAD, para los Adatos especialmente protegidos@ o *sensibles* durante el tratamiento informatizado (en especial las fases de recolección y comunicación o cesión) en el cual se requiere el consentimiento expreso y escrito para los datos que revelen la ideología, religión y creencias o, el mero consentimiento si los datos se refieren al origen racial, la salud y la vida sexual, cuando se refieren a los denominados ficheros de las Fuerzas y Cuerpos de Seguridad (art. 20-2 a 4), y particularmente, los ficheros con fines policiales.

La inaplicación se fundamenta en la denegación por parte de los responsables de los ficheros del ejercicio de los derechos de acceso, rectificación o la cancelación Aen función de los peligros que pudieran derivarse para la defensa del Estado o la Seguridad Pública, la protección de los derechos y libertades de terceros o *las necesidades de las investigaciones* que se estén realizando@ (art.21.1).

La norma cuestionada vulnera el Convenio de 1981 y el art. 18.4 CE. En efecto, el art. 9.2. del Convenio, estipula como excepciones *numerus clausus*, al

ejercicio de los derechos de habeas data (o de control de los datos de sí mismo), la seguridad pública o del Estado, los derechos y libertades de terceros, y la represión de las infracciones penales, con lo cual quedan por fuera las Anecesidades de las investigaciones@. Por consiguiente, la lectura constitucional del art. 21.1 LORTAD exige que el precepto, cuando alude a las ´necesidades de la investigación´ como excepción al ´*habeas data*´ sea interpretado en el sentido del Convenio de Europa de 1981, esto es, como necesidades de la investigación de determinadas y concretas infracciones penales [241]. Todo por incorporar términos indeterminados, difusos o vaporosos que conducen además a una quiebra del principio constitucional de seguridad jurídica (art. 93 CE.), que también se ve vulnerado por la norma recurrida.

2. Tratamiento informatizado de datos sensibles en ficheros de las Fuerzas y Cuerpos de Seguridad, sin consentimiento del titular (art. 20-3).

El artículo 20-3 de la LORTAD, se ha considerado el más polémico de cuantos se han recurrido por inconstitucionalidad ante el Tribunal Constitucional (TC), no sólo porque inaplica legislativamente el ejercicio del derecho de habeas data y el principio del consentimiento que tiene todo titular de los datos personales en un proceso informatizado, sino porque incide abierta, llana y gravemente sobre los *datos sensibles*, altamente protegidos por las legislaciones universales, comunitarias y estatales europeas.

En el art. 20-3 de la LORTAD, se posibilita el tratamiento informatizado de datos personales de la categoría de los sensibles o del *núcleo duro de la privacy*, sin el consentimiento del titular de los mismos cuando Asea absolutamente necesario para los fines de una investigación concreta@. Hace énfasis en la etapa inicial del tratamiento, es decir, en la recolección de datos personales sensibles por parte de las Fuerzas y Cuerpos de Seguridad del Estado. Se estima que con este proceder, la LORTAD, vulnera los arts. 18.4 y 16.2 de la CE, así como el Convenio Europeo de 1981, que proscribe todo tratamiento informatizado de datos personales de la

categoría de los sensibles, A a menos que el derecho interno provea garantías apropiadas@ (art. 6 *in fine*) , para cualquier fin, incluido el policial.

---

(241) Ibídem, pág. 309 y ss.

Sin embargo, sobre el particular hay discrepancia en la doctrina ibérica, pues se considera, por unos [242], que es factible el tratamiento informatizado de datos y obviamente su recogida, así sean datos sensibles de la persona, Aya que de otro modo sería prácticamente imposible el esclarecimiento de la mayoría de los casos investigados@. Otros [243], consideran que es inconstitucional el tratamiento informatizado de datos personales sensibles, más aún sin el consentimiento del titular, pudiera --sostienen-- justificarse dicho tratamiento de datos personales generales sin requisitos, Aya que los fines de una investigación concreta pueden entenderse incluidos en las excepciones del art. 9 del Convenio Europeo de 1981". No obstante, el Convenio como sostuvimos contiene unas excepciones *numerus clausus* entre las que no están las Ainvestigaciones concretas@ como causal de aquellas. En cambio, sí se menciona las Ainvestigaciones científicas@ o los datos personales Acon fines estadísticos@, siempre Aque no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas@ (art.9-3 Convenio) inmersas en las denominadas Arestricciones@ al ejercicio del derecho de información y el habeas data que tiene el titular de los datos en un proceso informatizado, pero no pueden interpretarse como investigaciones concretas (Preguntamos:)sobre qué, para qué y por qué?, pues los términos encierran una indeterminación conceptual y temática y por lo ambigua conduce a arbitrariedad de quie- nes las apliquen) ni tampoco son excepciones al ejercicio de derechos sino restricciones.

Unos y otros, concluyen al final, aún matizando sus considerandos que el art. 20-3, es inconstitucional porque vulnera el art. 18.4 en la medida que no hay justificación objetiva de que sea necesario la recogida de esos datos para la protección de la seguridad pública ni ningún otro bien jurídico constitucionalmente protegidos.

Más aún, la CE, no obliga a nadie a declarar sobre su ideología, religión o creencias (art.16-1); vale decir, que la persona no esta obligado a dar su consentimiento, ni nadie esta obligado a exigírselo sobre esta clase de datos personales considerados sensibles, tanto para revelarlos y con mucha mayor razón cuando se trate de someterlos

---

(242) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, A. Ob. ut supra cit., pág. 7.
(243) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 28

a un proceso informatizado o no de datos.

D. Comunicación (por cesión) interadministrativa de datos personales, sin consentimiento del titular (art. 19.1., en relación con el art. 6.2 y 11-2, e).

El art. 19.1 de la LORTAD, es inconstitucional, según el profesor *Morales Prats* [244], por vulnerar la garantía de reserva de la ley orgánica en el desarrollo de los derechos y garantías que derivan de la libertad informática (art. 18.4. CE). Igualmente, se inaplica legislativamente el principio del consentimiento del titular de los datos en las fases inicial o de recolección, comunicación e incluso de Auso@ de datos personales cuando se trata de ficheros de titularidad pública previstos en la LORTAD (arts. 18 y ss.), aún rebasando más las excepciones al consentimiento previstas en los arts. 6.2 y 11.2-e, de la misma LORTAD, excepciones que corren igual suerte de inconstitucionalidad que el art. 19.1. La rebaja de las garantías mínimas de los derechos y libertades fundamentales de la persona y del principio del consentimiento como una de aquéllas y previstas del Convenio Europeo de 1981, se ven reducidas a su más mínima expresión, pues lo deja inoperante; vale decir, inaplicable al tratamiento y A*uso*@ de los ficheros de titularidad pública. La inaplicabilidad o inoperancia del consentimiento del titular conlleva a un cierto determinismo de aquél por parte de las Administraciones Públicas, a tal punto que lo hace nugatorio y de paso desnaturaliza también el Aprincipio de la afectación@ [

245] de los datos previstos en el art. 5 del Convenio Europeo de 1981 y art. 4.2. de la LORTAD.

El recurrido artículo deniega la comunicación (por cesión) de datos personales interadministrativas de los datos personales recogidos o tratados por procesos informáticos por las Administraciones Públicas, Asalvo cuando la cesión hubiese sido

---

(244) MORALES PRATS, F. Ob. cit., pág.309 y ss

(245) APero, además, otra garantía básica de la libertad informática (art. 18.4), cual es la expresada en el art. 5 del Convenio del Consejo de Europa y en el art. 4.2.de la LORTAD, alusiva al principio de afectación (ligado al consentimiento del titular) del tratamiento automatizado de los datos personales a determinada finalidad, queda seriamente comprometida por el art. 19.1 LORTAD; este precepto posibilita la alteración de la finalidad del tratamiento de los datos (trámite cesión de los mismos), mediante normas de cobertura de carácter meramente reglamentario (cfr. Arts. 18.1 y 19.1 LORTAD)@. Cfr. MORALES PRATS, F. Ob. cit., pág.309 y ss

prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso@.

El principio del consentimiento, considerado nuclear en el proceso informatizado de datos español, contiene unas excepciones cuando se trata de ficheros de titularidad pública (art.6-2 LORTAD). En efecto, no se requerirá consentimiento, Acuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias@. Concordantemente el art. 11.2-e, no precisa el consentimiento del titular de los datos en la comunicación interadministrativa de los mismos en relación con los eventos del art. 19 LORTAD. Se deduce claramente que las excepciones están dirigidas exclusivamente a las fases inicial (recolección) y comunicación (por cesión) del tratamiento informatizado, pero además que la cesión estuviese prevista en la creación del fichero de titularidad pública respectivo y por disposición general publicada en el BOE o Diario Oficial correspondiente (art. 18-1 LORTAD) o por disposición posterior *que regule su uso* (art.19-1 in fine). Quizá por esto último, se diga que la inconstitucionalidad se acentúa más, porque la Administración tiene una carta blanca para poder entrecruzarse datos sin ninguna dificultad, obteniendo aquellos a los que, en

principio y debido a sus competencias, no les permitía acceder. No se trata de una delegación que el legislador hace en favor de la Administración, sino que supone una auténtica deslegalización que no se ajusta a límite o control alguno y, por ello, en franca contraposición a la reserva de ley recogida en el art. 53 CE [246].

4.4.4. 3. PRINCIPIO DE RESERVA DE LEY Y SEGURIDAD DE LOS DATOS: DERECHOS Y LIBERTADES FUNDAMENTALES (ARTS. 9-3, EN RELACIÓN CON EL ART. 7 Y EL ART. 17-1)

.

La LORTAD en varios artículos vulnera el principio de reserva de ley previsto en la Constitución Española (art.53-1) y por el cual, sólo por ley, que en todo caso deberá respetar el contenido esencial, podrá regularse el ejercicio de derechos y libertades

---

(246) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, A. Ob. ut supra cit., pág. 7.

fundamentales reconocidos en el Capítulo II del Título Primero de la CE, y dentro de los cuales está el derecho a la intimidad, el honor, la imagen, etc. La tutela de dichos derechos y libertades se ejercerá mediante recurso de inconstitucionalidad ante el Tribunal Constitucional (art. 161-1,a). En este aparte nos ocuparemos de dos artículos: el art. 9-3 y el art. 17.1., LORTAD.

Principio de seguridad de los datos personales de categoría sensible (ar.9-3).

El art.9-3 LORTAD, establece que mediante Reglamento se establecerán los requisitos y condiciones que deben reunir los ficheros informatizados y las personas que intervengan en el proceso informatizado de datos personales sensibles.

Hemos sostenido, que la legislación universal, y en particular, la Comunitaria Europea, proscribe el sometimiento a proceso informatizado los datos considerados sensibles, salvo que existan garantías idóneas de protección plena, clara y

precisamente establecidas en el ordenamiento jurídico de cada Estado (art. 6 Convenio de 1981). Este principio que también se ha denominado APrincipio General de Interdicción@, palmariamente se halla vulnerado por el art.9-3, cuando establece que será por AReglamento@ y no por Ley (al menos Ordinaria y de menor entidad que la Ley Orgánica) la regulación de requisitos y condiciones que deben reunir los ficheros como las personas que intervienen en el tratamiento informatizado de datos personales de la categoría de los sensibles. Así, se vulnera concomitantemente el art. 53-1, CE, por quebrantar el principio de reserva legal, al dejar en manos del Reglamento, materias o aspectos atinentes a los derechos y libertades fundamentales, que sólo están reservadas exclusiva y excluyentemente a la ley, derechos tales como los previstos en el art. 18.4 CE.

B. Tutela de los derechos fundamentales en el tratamiento informatizado de datos (art. 17-1).

La LORTAD, establece que las actuaciones contrarias a las fases de tratamiento informatizado de datos o de los derechos fundamentales que éstas involucran, pueden ser objeto de reclamación por los titulares de los datos personales ante la Agencia de Protección de Datos, A*en la forma que reglamentariamente se determine@.* (art.17-1 *in fine*).

La LORTAD, quebranta el principio de reserva de ley previsto en la CE (art.53-1), en relación con el art. 18.4 y 24.1 CE, cuando en el art. 17.1, remite a una norma de rango inferior (El Reglamento), la Ley de regulación procesal de los Recursos contra actuaciones de los poderes públicos contrarias a ésta [247]. En efecto, con la remisión se involucra aspectos procesales importantes como los eventuales recursos que se desatarían ante la Agencia de Protección de Datos, por desconocimiento o quebrantamiento de derechos y libertades fundamentales previstos en la regulación del tratamiento informatizado de datos de la LORTAD, que siendo objeto de la ley exclusivamente se trasladan al Reglamento.

4.5. LAS DIRECTIVA 95/46/CE Y 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 1995 Y 1997, RESPECTIVAMENTE.

Los recursos de inconstitucionalidad *sub júdice* contra la LORTAD ante el Tribunal Constitucional, como se ha sostenido se ven tocados no sólo por la expedición de normas comunitarias previas, como el Convenio de Estrasburgo de 1981, sino posteriores a su planteamiento, como la Directiva 95/46/CE, pero previa a la resolución de los recursos. La incidencia jurídica deviene de la transposición normativa [248] que de la Directiva Comunitaria, debe hacer el Estado Español, el 31 de Octubre de 1998, como fecha límite, según la disposición final prevista en el art. 32.1, para que la normativa existente (LORTAD y R.D., que la desarrollan) o las reformas legislativas idóneas (Proyectos que ya cursan en las instancias legislativas [249]) en materia de protección de las personas físicas cuando sometan a tratamiento informatizado sus datos

---

(247) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 25

(248) Un estudio de los impactos de la transposición normativa en Bélgica con conclusiones comparativas a la transposición de la Directiva de protección de datos en España, puede consultarse, en: DUMORTIER, J. Y ALONSO BLAS, Diana.*LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION DE DATOS EN BELGICA.* En: Actualidad Informática Aranzadi. Ed. Aranzadi, Núm. 20. Julio, Pamplona, 1996, págs. 1-7 y ss.

(249) Un breve comentario al anteproyecto de reforma a la LORTAD, en GUTIERREZ SANCHEZ, Pedro. *ANTEPROYECTO DE LEY ORGANIZA POR LA QUE SE MODIFICA LA LEY ORGANICA 5/1992, DE 29 DE OCTUBRE, DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL (LORTAD).* En: Actualidad Informática Aranzadi. Ed. Aranzadi, Núm. 20. Julio, Pamplona, 1996, págs. 1-4 y ss.

personales se adopten de conformidad con las previsiones de tutela y garantía prevista en la Directiva.

Por ello, haremos un estudio sucinto de los aspectos capitales que plantea la Directiva, y sobre todo, aquellos que hacen referencia a los principios, derechos y garantías de los titulares de los datos personales generales y sensibles y las fases del proceso informatizado de los datos mismos. Así mismo, se hará referencia puntual a una reciente Directiva Comunitaria que incide en la fase de comunicación del proceso informatizado de datos y en los principios y garantías de tutela de los

titulares de los datos personales; nos referimos a la Directiva 97/66/CE, *relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas.*

4.5.1. LA DIRECTIVA 95/46/CE, sobre *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

La Directiva 95/46/CE., en materia de *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* contiene una estructura normativa *sui géneris* muy propia de las normas comunitarias europeas, pertenecientes a las fuentes del llamado Derecho Derivado Comunitario [250]

La Directiva esta dividida en dos grandes partes: una, de carácter interpretativo o hermenéutico; y otra, de carácter normativo propiamente dicho, y por ende con efectos

---

(250) Este derecho escrito es el creado por los organismos comunitarios (El Parlamento, La Comisión y El Consejo, especialmente). Comprende en primer término, los actos jurídicos expresamente previstos en los Tratados de creación de la CE (hoy UE, Unión Europea); actos que contienen reglamentaciones obligatorias para los Estados Miembros. Estos son: los Reglamentos, LAS DIRECTIVAS, y las Decisiones dirigidas a particulares y al Estado Respectivo; así como las Recomendaciones o razones que emanan del Tratado de la CECA, y los Acuerdos Internacionales que conciernen a la Comunidad Europea. Mis trabajos: *LAS FUENTES DEL DERECHO COMUNITARIO EUROPEO.* En: Revista FORO UNIVERSITARIO. Ed. UNED, Univ. de Nariño, Núm. 15, Pasto, 1988, pág.65-75; y, *LOS DENOMINADOS RECURSOS ANTE LOS TRIBUNALES DE JUSTICIA DE LA C.E Y ANDINO.* Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, pág. 11 y ss.

jurídicos, dividida en capítulos, secciones y artículos. La primera parte, contiene un amplísimo número de considerandos, 72 en total, los cuales constituyen la exposición de motivos de la norma jurídica; vale decir, la parte de interpretación hermenéutica plasmada por el propio legislador comunitario a fin de desentrañar y justificar el cuerpo del texto normativo. En dichos considerandos está el espíritu y

razones de ser de la norma comunitaria, por ello, en el transcurso de esta investigación haremos referencia a aquéllos.

La segunda parte, se estructura así: Capítulo I. *Disposiciones Generales*: Objetivo de la Directiva (art.1), Definiciones (art.2), Ambito de aplicación (art.3), Derecho nacional aplicable (art.4). Capítulo II. *Condiciones generales para la licitud del tratamiento de datos personales:* Secc. I. Principios Relativos a la Calidad de datos (art. 6). Secc. II. Principios Relativos a la Legitimación del Tratamiento de datos (art. 7). Secc. III. Categorías Especiales de tratamiento (arts.8 y 9). Secc. IV. Información del interesado (arts.10 y 11). Sec. V. Derecho de Acceso del interesado a los datos (art.12). Secc. VI. Excepciones y limitaciones (art.13). Secc.VII. Derecho de Oposición del interesado (art. 14 y 15). Secc. VIII. Confidencialidad y Seguridad del Tratamiento (arts. 16 y 17). Sec. IX. Notificación (arts. 18 a 21). Capítulo III. *Recursos Judiciales, Responsabilidad y Sanciones* (arts. 22 a 26). Capítulo IV. *Códigos de Conducta* (art.27). Capítulo VI. *Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales* (arts. 28 a 30). Cap. VII. *Medidas de ejecución comunitarias* (art. 31). *Disposiciones Finales* (art.32 a 34).

Los principios de protección a las personas físicas (identificadas o identificables, no anónimas [251]) en el tratamiento informatizado o manual (aunque sólo extensible a los denominados *ficheros* no a las *carpetas* de datos) [252] de datos personales, pre-

---

(251) En similar sentido, los considerandos 25, 26, 68 y 72 de la Directiva.

(252) Según el considerando 27, ALa protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su *tratamiento manual*; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los *ficheros*, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva@.

vistos en la Directiva, tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias

u otros organismos que efectúen tratamientos. Estas obligaciones, se refieren en particular, a la calidad de datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento. De otra parte, estos principios hacen referencia a los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, tales como, el de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias [253].

4.5.1.1. GLOSARIO DE TERMINOS IUSINFORMATICOS: DEFINICIONES TECNICO-JURIDICAS.

En tal virtud, y antes de abordar el análisis referencial de los principios de protección de los titulares de los datos personales, hagamos referencia a las definiciones de los conceptos aplicables al tratamiento informatizado de datos, pues éstas constituyen el glosario indispensable para el entendimiento jurídico-técnico de la Directiva, y lo que es más importe aún, conducen a una mejor interpretación hermenéutica de los conceptos básicos para el tratamiento de datos personales, que tienen por objeto garantizar el respecto a los derechos y libertades fundamentales, en particular en derecho a la intimidad, reconocido en el Convenio Europeo para la protección de Derechos Humanos y de las Libertades Fundamentales (art. 8), así como en los principios generales del Derecho Comunitario y el Convenio de 28 de Enero 1981, que protege el conjunto de derechos y libertades fundamentales (incluido la intimidad) en el curso de un tratamiento informatizado, precisado y ampliado por la Directiva en éstos menesteres (C. 10 y 11).

En efecto, *Datos personales*, se considera *toda información sobre una persona*

---

(253) Para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identi- ficar a dicha persona. Por tanto, los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado. Los códigos de conducta

con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado (Considerando 26).

física identificada o identificable (el interesado); se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (art.2-c). Esta definición, incorpora elementos de forma y de fondo empleados en la identificación plena de una persona humana, a efectos de evitar al máximo el error, la indeterminación o la confusión del titular de unos datos personales que le conciernen o le puedan concernir si se reputa identificable directa o indirectamente, o lo que es lo mismo, la persona interesada. Esta definición cualificada de persona física a la que le corresponde una información de carácter personal, elimina las dificultades generadas en torno identificabilidad, no sólo por medios documentales tradicionales (DIN o DNI, etc), sino por elementos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; vale decir, por las caracteres relevantes de la identidad heredo-biológica de la persona, su hábitat social y cultural y hasta su nivel socio-económico. Se crea así una especie de derecho a la identificación como garantía de los derechos fundamentales asignados a una persona humana, cuando sean sometidos a tratamiento informatizado o manual datos personales.

Los distintos elementos característicos definidores de la identidad de una persona permiten además, a los Estados Miembros de la UE, estructurar en su normas reguladoras de la protección de derechos y libertades fundamentales y del proceso informatizado de datos personales, según se sostiene en el C. 27, de la Directiva, que se regule, entre otros aspectos importantes, el ejercicio del derecho de *habeas data*, en particular, el derecho acceso a dicho conjunto de datos; así mismo que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la Directiva 95/46/CE.

El *Tratamiento de datos personales*, se considera a *cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicables a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción* (art.2-b). Esta definición cualificada, a diferencia de la actividad rehusada por el grupo de expertos del Convenio de 1981 para hacerlo, conlleva unos elementos técnicos, jurídicos y acciones informáticas con los denominados archivos o registros informáticos (o *file*), incorporados o por incorporar en una base de datos (*database*) o ficheros informatizados (*fichiers*), que en su conjunto conforman el proceso o Aprocedimiento automatizado@ de datos personales.

En efecto, son etapas o fases de un procedimiento informatizado de datos, la recolección, almacenamiento, registro, conservación y comunicación (por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión. Aspectos técnicos idóneos que posibilitan el nuevo fenómeno tecnológico de la comunicación y la información : TIC). Las acciones de consulta, extracción, bloqueo, supresión o destrucción, modificación incorporadas en la definición de tratamiento de datos personales, que bien pueden hacerse con medios informáticos, electrónicos o telemáticos sobre archivos o registros (o simplemente datos) contenidos en ficheros informatizados o bien con medios mecánicos o manuales en ficheros de idéntica índole, engloban el concepto genérico de Atratamiento@ previsto en la Directiva en forma multicomprensiva.

El *Fichero de datos personales*, se entiende *todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado o repartido en forma funcional o geográfica* (art. 2-c).

Cabe resaltar de la definición que los Acriterios determinados@, son aquellos establecidos en la correspondiente normativa estatal sobre el tratamiento informatizado de datos personales, el ámbito de aplicación de dicha normativa, y sobre todo, los elementos característicos de la persona identificable que antes puntualizábamos, pues ellos indicarán la menor o mayor cobertura de protección de los derechos y libertades fundamentales de la persona. Una normativa miope en éstas lides sería la que estipula la identificabilidad de la persona por el sólo criterio documental v.gr. El D.N.I. o DIN.

En igual forma, la definición *fichero* amplía los criterios de ámbito de aplicación de la normativa a los aspectos de distribución de competencias por servicios (centralizado o descentralizado), territorial (o geográfico) y funcional, teniendo en cuenta la estructura estatal de los Estados Miembros de la UE (Estados Unitarios, Federales o Comunitarios, como el Español).

El *Responsable del tratamiento*, es quizá con el de Atratamiento de datos personales@ dos de los conceptos más elaborados en la Directiva, por su íntima correspondencia temática, los efectos jurídicos y materiales y las implicaciones en los ámbitos de tutela, garantía, régimen de responsabilidades y sanciones y derechos y deberes de los sujetos intervinientes en el proceso o procedimiento informatizado (el titular de datos, Aencargado del tratamiento@ [254], el responsable del fichero, Ael tercero@[255] y Ael destinatario@ [256]).

Así, se considera *Responsable del Tratamiento* (institución jurídica más amplio y precisa que la de Aresponsable del fichero@, utilizada por la LORTAD [257]), es *la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo* _____

(254) El Aencargado del tratamiento@, es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento (art. 2-e)

(255) El ATercero@, es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento (art. 2-f).

(256) El A*Destinatario*@, es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que

puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios (art. 2-g).

(257) En la Doctrina Ibérica, se ha sostenido la deficiente definición de la figura del responsable del fichero realizado por la LORTAD; entre otras, por las siguientes razones: a) la determinación de este sujeto se realiza conforme a *varios criterios*, sin determinar cuál es de aplicación en cada caso, por lo que se plantea el problema de si el titular del fichero puede optar entre uno u otro criterio a la hora de señalar quién es dicho responsable --con la consiguiente posibilidad de manipulación y utilización estratégica de las distintas posibilidades que se contienen en la definición legal del responsable del fichero, para eludir la propia potestad sancionadora con el correlativo compromiso de la funcionalidad general del sistema--; b) la particular y no menos deficiente descripción del responsable del fichero en el ámbito público que determina la imposibilidad de aplicar los criterios legalmente previstos a determinados ficheros que, por el contrario, sí se encuentran sometidos al ámbito de aplicación de la ley --como es el caso de los órganos constitucionales-- que por su especial estructura jurídica no tienen fácil acomodo en ninguna de las categorías contempladas en la definición legal; y, c) la falta de distinción entre el responsable del fichero y el encargado del tratamiento, sujeto que, sin perjuicio de realizar actividades con indudable incidencia en el campo que analizamos --que determinan su sumisión específica al deber de guardar secreto (art.10 LORTAD)-- no se encuentre sujeto a responsabilidad alguna. Vid. DE LA SERNA BILBAO, María Nieves. *LA AGENCIA DE PROTECCION DE DATOS ESPAÑOLA: CON ESPECIAL REFERENCIA A SU CARACTERISTICA DE INDEPENDENCIA*. En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 22 de Enero, Pamplona, 1997, pág. 3

que sólo o conjuntamente con otros determine los fines y los medios de tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario (art. 2-d).

A través de la naturaleza jurídica y funciones genéricas y específicas del responsable del fichero en el transcurso del procedimiento informatizado de datos, se logra caracterizarlo, tal y como lo delinearon los legisladores comunitarios. En efecto, aquélla y algunas de éstas, son:

a) *Naturaleza jurídica*: La Directiva deja al ámbito legislativo de los Estados la determinación de sí, el responsable del tratamiento debe tener una misión de interés público o inherente al ejercicio del poder público, o si debe ser una administración pública u otra persona de derecho público o privado (considerando 31). La amplitud de la naturaleza jurídica del responsable del tratamiento identifica el amplio o reducido abanico de funciones, derechos, obligaciones y niveles de responsabilidades que debe asumir aquél. v.gr. En la transmisión de un mensaje con datos, a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de este tipo, será considerado responsable del tratamiento de datos, aquélla persona de quien procede el mensaje y no la que ofrece el servicio de transmisión **[258]**.

b) *Ambito de Aplicación*. Serán aplicables los principios de protección de datos previstos en la Directiva, a todos los tratamientos de datos (total o parcialmente informatizados, así como a los informatizados siempre que puedan ser incluidos en un fichero) en los cuales las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho Comunitario, salvo que expresamente estén excluidas [259].

---

(258) Sin embargo, pueden reputarse, llegado el caso, en responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio) (Considerando 47, *in fine*).

(259) Se excluyen: a) El ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho co- munitario, como las previstas por las disposiciones de los títulos V y VI, del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de fatos que tenga por objeto las seguridad pública, la defensa, la se-
guridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del mismo Estado en materia Penal; y, b) Los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. v.gr. La correspondencia y llevanza de un repertorio de direcciones (Art. 3-2., conc. con el considerando 12).

c) *Identificabilidad de una persona*. A efecto de aplicar el sistema de protección arbitrado para las personas, en particular el derecho de información que a ésta le asiste como persona identificada o identificable, el responsable del fichero deberá tomar para determinar la identificabilidad de la persona, el Aconjunto de los medios que puedan ser razonablemente utilizados@ por éste o por Acualquier otra persona@, para identificarla (C. 26).

d) Limitación de las funciones, por excepciones *numerus clausus*. Los Estados en sus legislaciones internas, pueden imponer restricciones a determinadas obligaciones del responsable del tratamiento, cuando sean necesarias para salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas (C. 43);

e) *Funciones por encargo*. Para evitar que una persona quede excluida de la protección garantizada por la Directiva, será necesario que los Estados prevean que

cualquier persona que efectúe tratamientos de datos, por cuenta del responsable (Aencargado del tratamiento@) actúe bajo la autoridad y responsabilidad del responsable del tratamiento establecido en cada legislación estatal (C. 18).

El responsable o encargado del tratamiento no serán dispensados de las demás obligaciones que les conciernen conforme a la Directiva o la normativa estatal correspondiente, diferentes a los de notificación a los sujetos involucrados en el tratamiento informatizado de datos, en aquellos casos, por ejemplo, que tengan como fin evitar trámites administrativos improcedentes o innecesarios en torno a la exención o simplificación de la notificación para los tratamientos de datos, siempre que no atenten contra los derechos y libertades de los interesados (C. 49 y 51).

f) *Recurribilidad de los Actos del Responsable del tratamiento*. A fin de que se respeten los derechos de los interesados por parte de los responsables de los ficheros, los Estados en sus legislaciones arbitrarán un A*recurso judicial*@. Los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor (C. 55);

g) *Funciones de garante en la comunicación de datos.* Podrán adoptarse Amedidas particulares@ para paliar la insuficiencia del nivel de protección de un tercer país, siempre que el responsable del fichero ofrezca Agarantías adecuadas@ en la comunicación de datos personales entre Estados (AFlujos internacionales@), previos la existencia de instrumentos legales y procedimientos de negociación entre la Comunidad y los países terceros, sobre la materia (C. 20 y 59).

4.5.1.2. PRINCIPIOS FUNDAMENTALES APLICADOS A LAS FASES DEL PROCEDIMIENTO INFORMATIZADO DE DATOS PERSONALES.

4.5.1.2.1. NOTAS PRELIMINARES AL SISTEMA DE PRINCIPIOS.

El sistema de principios fundamentales en el procedimiento informatizado de datos personales con vista a la Directiva 95/46/CE, contiene unas directrices de interpretación hermenéutica previstas en los considerandos (C), a saber:

a) Las legislaciones estatales que regulan el tratamiento informatizado de datos personales, tienen por objeto garantizar el respeto de los derechos y libertades fundamentales (incluido el derecho a la intimidad) y los principios generales del Derecho Comunitario. En consecuencia, la aproximación de dichas legislaciones a las directrices de la Directiva, no deben conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la UE (C.10).

b) Los principios de protección de los derechos y libertades de las personas, precisan y amplían los del Convenio Europeo de 1981 (C.11).

c) Los principios se aplican a todos los tratamientos (total o parcialmente informatizado, incluso los manuales cuando los datos están contenidos o destinados a ser incluidos en un fichero) de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito del Derecho Comunitario. La exclusión es taxativa, vale decir, *numerus clausus* --art. 3-2-- (C.12)

d) Los principios de protección se aplicarán en forma restringida en los tratamientos de sonido y de la imagen [260] con fines periodísticos o de expresión literaria o artística (C.17) [261]. Es decir, que los principios de protección de las personas en un procedimiento informatizado de datos se aplicarán en la medida que resulten necesarios para la conciliación del derecho a la intimidad con las normas que rigen la libertad de expresión.

e) Los principios tienen su expresión en dos ámbitos correlacionados, a saber: uno, las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos (v.gr. calidad de datos, seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento); y otro, los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su trata-

---

(260) Como lo confirman Dumortier y Alonso Blas, ASi bien la Ley Orgánica no aludía en concreto a dichos conceptos, sí se aludía a los mismos en el art. 1-4 del Reglamento de la Agencia (D.R.1332/1994, de 20 de Junio) -- información fotográfica, acústica o de cualquier otro tipo). En todo caso, en la Directiva se amplía más el dato personal de imagen al incluir no sólo la captada por aparato fotográfico, sino también por videocámaras y, en definitiva, por lo que puede definirse como sector audiovisual (agregaríamos con medios informáticos, electrónicos o telemáticos que manejan el dato personal de imagen, tal como precisaremos en la parte III y IV de esta investigación). No cabe duda que la utilización de imagen y sonido ha experimentado un gran aumento : controles de acceso a edificios, fichero de policía, utilización de la voz en el automóvil o de la imagen en controles de acceso en autopistas, en detección de infracciones de tránsito, en los servicios y comercio mediante los terminales de información, en el mundo del trabajo y de las relaciones profesionales, en el ámbito del hogar o en el terreno de la salud. El reconocimiento de la voz y el sonido como datos personales efectuado por la Directiva va a potenciar la protección de los mismos en aras de la salvaguarda de la intimidad personal (o mejor al conjunto de derechos y libertades fundamentales previstos en la CE, en el ámbito español)...@ DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION DE DATOS EN BELGICA.* En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 20 de Julio, Pamplona, 1997, pág. 5

(261) Conforme al art.9 de la Directiva, los Estados aplicarán A*exenciones* y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad expresión@, cuando se trate de la aplicación de los Capítulos (IV), ATransferencia de datos personales a países terceros@ y Capítulo VI, AAutoridades de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales@.

miento en determinadas circunstancias (C.25). Huelga decir, los derechos estructurales del ejercicio del derecho de *habeas data* y el derecho de oposición al tratamiento informatizado de datos por parte de los titulares, previstos en los arts. 10 a 12 y 14 de la Directiva, respectivamente. Derechos base y fundamento de la visión iusinformática de los derechos y libertades fundamentales, como hemos visto.

f) Los principios de protección se aplican a cualquier información relativa a una persona identificada o identificable (art. 2-a Directiva). Por contra, no se aplicarán a los datos hechos anónimos de tal manera que ya no sea posible identificar al interesado (C.26); y,

g) El Sistema de principios de protección de los derechos y libertades de las personas, según el C.68, no es un sistema acabado, puesto que los Estados podrán completar y precisarlo, Asobre todo en determinados sectores, mediante normas específicas conforme@ a los principios previstos en la Directiva.

Ahora bien, los principios de protección de los titulares de los datos previstos en la Directiva, aplicados a las diferentes fases del proceso informatizado de datos, que a la vez las estructuran y dan contenido, las podemos clasificar y enunciarlos así: a) Fase de recolección de los datos; b) Fases de almacenamiento, registro y conservación de los datos; y b) Fase de Comunicación de los datos.

Sin embargo, como principio directriz de todo el procedimiento total o parcialmente informatizado o manual, siempre que los datos vayan a constituir parte de un fichero, la Directiva a erigido como actividad ineludible y de resorte del responsable del tratamiento, o en su caso, su representante, el que denominaremos *principio previo de notificación a la autoridad de control*, prevista en el art.28 de la Directiva. Esta autoridad de control, como autoridad pública, encargada de vigilar la aplicación en cada territorio estatal de las disposiciones de la Directiva, que tiene como objetivo primordial, la protección de los derechos y libertades fundamentales de las personas físicas en lo que se refiere al tratamiento de datos personales, con funciones atribuidas con total independencia y con poderes de investigación, poderes efectivos de intervención y con capacidad procesal en caso de infracciones a la Directiva. Las decisiones de esta autoridad que causen lesión a los derechos serán objeto de recurso jurisdiccional (art. 28 Directiva).

Con fundamento en este principio fundamental previo al tratamiento de datos personales, el responsable del tratamiento o, en su caso, su representante efectuarán una notificación a la autoridad de control, siempre que dicho tratamiento vaya destinado a la consecución de un fin o de varios fines conexos.

La notificación, como uno de los *mecanismos de control* previo que deben adoptar los sujetos involucrados en iniciar un tratamiento de datos personales para eludir cualquier suposición de riesgo para los derechos y libertades de las personas deberán velar porque se cumpla a cabalidad Aantes del comienzo del tratamiento@ (art.20. Ibídem).

La notificación contiene como mínimo la siguiente información: a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; b) el o los objetivos del tratamiento; c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento; d) los destinatarios o categorías a los que se pueden comunicar los datos; e) las transferencias de datos previstas a países terceros; f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas con motivo de la seguridad del tratamiento (art.17 Directiva) resultan adecuadas para garantizarlo.

4.5.1.2.2. FASE INICIAL O DE RECOLECCION DE DATOS.

En la *Fase inicial o de Recolección de datos*, se aplicarán algunos de aquellos principios relacionados en el grupo de principios relativos a la Acalidad de los datos@ (art. 6), el grupo de los principios relativos a la Alegitimación del tratamiento de los datos (art.7) y en las ACategorías especiales de tratamiento@ de los datos (art.8) de la Directiva. Valga decir, que varios de los subsiguientes principios no sólo se aplican a la fase de recolección de datos, sino a todo el procedimiento informatizado, tal como lo anotaremos puntualmente al comentar cada uno de estos. En efecto, estos son:

a) *El principio de compatibilidad de la recolección de los datos con las finalidades del tratamiento*. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento

posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías adecuadas (art. 6-b).

b) *Principio de proporcionalidad (pertinencia, adecuación y no excesibilidad) de los fines*. Los datos que se recaben (o recojan) deben guardar la proporcionalidad de esta actividad con los fines de tratamiento posteriores, es decir, que deben ser adecuados, pertinentes y no excesivos en relación con dichos fines (art. 6-c).

c) Principio de lealtad y licitud. Este principio, también conocido como de legalidad (que no legitimidad, como se suele confundir [262]), es aplicable a todo el tratamiento informatizado de datos personales, y obviamente a la etapa inicial del proceso conocida como de recolección de datos. En tal virtud, toda recolección de datos personales deberá hacerse de conformidad con el ordenamiento jurídico vigente sobre la materia en cada Estado, siguiendo para ello las directrices previstas en la Directiva. Es decir, que el tratamiento sea lícito. Si una persona sufre un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE., aquella tendrá derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. Según el art. 23-2 de la Directiva, el responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

---

(262) En este sentido, se mencionan los principios relativos a A*la legitimidad del tratamiento de datos*@ (art.7 Directiva), como una explicación del principio de lealtad y licitud de los datos (art.6-1 Ibídem). BETES DE TORO, Alfredo. *El DERECHO DE INFORMACION Y LOS PRINCIPIOS LEGITIMADORES DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARACTER PERSONAL EN LA DIRECTIVA 95/46/CE, DE 24 DE OCTUBRE DE 1995*.En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 25 de Octubre, Pamplona, 1997, pág. *7*

Que el tratamiento de datos sea leal, supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención (C.38).

d) *Principio de veracidad y exactitud de los datos*. Los datos personales que se recaben deben responder a la verdad y exactitud vertida por los titulares de la misma, tanto si ha sido recolectada del propio interesado como si no fuesen recabados de éste.

Los sujetos involucrados en el tratamiento de datos, principalmente el responsable o encargado del tratamiento, deberán tomar las medidas razonables para que los datos no sean inexactos o incompletos; y llegado el caso, si lo fuesen y contrarían además el principio de la proporcionalidad de la recolección con los fines, puedan posteriormente ser suprimidos o rectificados, tras el ejercicio del *habeas data* (acceso, rectificación, actualización y cancelación) por parte del interesado.

e) *Principio de legitimidad de la recolección de datos*. Este principio es de capital importancia en la protección de derechos y libertades fundamentales, y en particular de la intimidad, cuando los datos personales sean sometidos a procedimiento informático.

Además, éste principio engloba otros que se consideran estructurales o continentes de éste, tales como el principio del consentimiento (columna vertebral de la LORTAD), el principio de finalidad del tratamiento de datos y el de prevalencia de ciertos intereses en el tratamiento de datos, tales como, los intereses vitales para el interesado, el interés público para los poderes públicos o los intereses legítimo para el responsable del tratamiento. Quizá por ello, el concepto jurídico de legitimidad rebasa al de la simple legalidad, pues aquélla es más amplia y de aplicación *erga omnes* a los sujetos involucrados en el tratamiento de datos personales, pues está fundada en criterios de la legalidad, de valores o de intereses públicos o particulares, y no simplemente normativos como es el caso de la legalidad.

Este principio de la legitimidad del tratamiento [263] se aplica a todo el tratamiento de los datos, y por obvias razones, a la primera fase inicial o de recogida de datos. En tal virtud, siendo la legitimidad más amplia y genérica que la legalidad, pero ambas dirigidas a la protección de derechos y libertades fundamentales , la Directiva 95/46/CE, establece unas líneas directrices que legitiman el tratamiento de datos. Estos son:

1. El *principio del consentimiento* que requiere para todo el tratamiento de datos, y en particular, para la etapa inicial de recolección de la información. El consentimiento del interesado o titular de los datos deberá ser en forma inequívoca y explícita, salvo las excepciones *numerus clausus* previstas en la Directiva cuando se trata de Acategorías especiales de datos@ (art. 8-1 a 8-3, Directiva) [264].

2. *El principio de finalidad de los datos*. Principio que se estructura en las siguientes eventualidades: a) Cuando el tratamiento es necesario para la ejecución de un contrato en el que sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; y, b) Cuando el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.

3. *El principio de prevalencia de ciertos intereses públicos y particulares*. Este principio se presenta en los siguientes eventos: a) Cuando sea necesario para proteger un *interés vital* del interesado; b) Cuando sea necesario para el cumplimiento de una misión de *interés público* o inherente al ejercicio del poder público conferido al respon-

---

(263) Se ha considerado de tal importancia este principio (aunque se los autores hablan de principio de legalidad), que comentan que el legislador belga, al abordar el tema de la transposición de la normativa Comunitaria (Directiva 95/46/CE), Atiene la intención de incluir literalmente el texto del artículo 7... en el nuevo proyecto de ley de protección de datos. El motivo de esta transposición literal se funda en el concepto de Directiva como instrumento de Derecho Comunitario que autoriza a los Estados Miembros para decidir la forma y medios para su cumplimiento, pero les obliga en forma estricta en cuanto a su contenido@. Al fin y al cabo, como antes sostuvimos la Directiva es una norma jurídica comunitaria de carácter obligatorio para

los Estados Miembros, pues pertenece a las fuentes del llamado ADerecho Derivado Comunitario@ Cfr. DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION*... Ob. cit., pág. 8.

(264) En dicha categoría se incluyen los denominados por la doctrina anglosajona como los datos del Anúcleo duro de la privacy@ (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad) -- Art.8-1--; En cuanto a las excepciones taxativas, giran en torno al concepto del consentimiento explícito e inequívoco del interesado o titular de los datos personales.

responsable del tratamiento o a un tercero a quien se comuniquen datos; y, c) Cuando sea necesario para la satisfacción del *interés legítimo* perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que prevalezca el interés o los derechos y libertades fundamentales del interesado que requie- ran protección, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de datos personales.

f) *El principio de interdicción de tratamiento de datos personales pertenecientes a las ACategorías Especiales*@. La regla general, es la prohibición del tratamiento respecto de los datos personales inmersos en la categoría de especiales (que incluye a los denominados datos Asensibles@ o hipersensibles, comentados por la doctrina ibérica **[265]**)que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. La interdicción al tratamiento se funda en la naturaleza de los datos personales, los cuales pueden atentar contra los derechos y libertades fundamentales, y en especial, contra la intimidad, las cuales *a priori* no deber ser objeto de tratamiento alguno (informatizado o manual) de datos .

La excepción a la regla la constituye el consentimiento inequívoco y explícito del interesado o titular de los datos personales. Las excepciones taxativas **[266]** o, *lista* _____

(265) Veáse, p.e., en la obras citadas ut supra, a CASTELLES ARTECHE, SOUVIRON, FAIREN GUILLEN, ORTI VALLEJO, MORALES PRATS, BAJO FERNANDEZ, en las visiones de aquellos datos sensibles, hipersensible y aún con plus especial de hipersensibilidad en materia constitucional, administrativa, civil y penal, respectivamente. En la parte III y IV, de la investigación ahondaremos más sobre el tema.

(266) Las excepciones son: a) Cuando el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho Laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas; b) Cuando el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente

incapacitado para dar su consentimiento; c) Cuando el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por un fundación, una asociación, o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados; d) Cuando el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) Cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por una profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto (art. 8-3); f) Cuando el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer

cerrada de datos [267] exceptuados, pero al fin y al cabo lista considerablemente amplia y posibilitadora de acrecentamiento por Amotivos de interés público importantes@ (art.8-4), o por Adisposiciones nacionales que prevean garantías apropiadas y específicas@ en materia de datos relativos a infracciones, condenas penales o medidas de seguridad (art.8-5 *ab initio*) en la Directiva y fundada en criterios de legitimidad (derechos, valores, intereses públicos y privados) y no de simple legalidad. Estas causales de excepciones maleables en cada Estado Miembro, como medida de control de la UE, deberán ser notificadas a la Comisión, si se llegaren a adoptar en las legislaciones internas respectivas (art.8-6).

Quizá tal vez, por esa amplitud y acrecentamiento de excepciones, se pueda pensar metafóricamente que la regla prohibitiva al tratamiento de datos, constituye el prisma del cual se refleja un arcoiris de excepciones, que por serlas siguen teniendo como referente a la regla, pero con cierto temor fundado de desvirtuarla. Muy a pesar, se piensa por un sector de la doctrina hispana [268] , que aún teniendo la lista de excepciones un Acarácter limitativo@, pero ampliable por cada Estado Miembro de la Comunidad --en nuestro sentir demasiado amplísima, aún considerando los fundamentos de las excepciones basadas en la heterogeneidad de los Estados Miembros de la Comunidad que propenden al ser UE., por una homogeneidad, al menos legisla-tiva-- resulte un punto poco claro que, basándose en declaraciones incluidas en el acta de la sesión del Consejo en que se aprobó la posición común de la Directiva, se afirme en buena lógica que los Estados miembros

podrán precisar o concretar las categorías de datos calificados como sensibles, teniendo en cuenta las características jurídicas y socio-

---

----Continuación nota 266---

el Estado Miembro basándose en las disposiciones nacionales que prevean garantías apropiadas y específica. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos (art. 8-5 *ab initio*); g) Cuando el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos (art. 8-5 *in fine*); h) El Anúmero nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento@, si los Estados UE, así lo consideran en condiciones especiales (art.8-7). Texto completo en la dirección electrónica: WWW. CC.CEC (DATABASE CELEX).

(267) DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION DE LA DIRECTIVA...* Ob.cit., pág. 9

(268) Ibídem, pág. 9 y 11. Cita para corroborar su argumento a HEREDERO HIGUERAS, M., *LA LEY ORGANICA 5/1992, DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARACTER PERSONAL: COMENTARIO Y TEXTOS.* Ed. Tecnos, 1996, pág. 99.

lógicas de cada país. La Dirección General XV de la Comisión Europea ha confirmado en todo caso el carácter limitativo de esta lista, afirmando que las mencionadas declaraciones incluidas en las actas del Consejo *no tienen valor jurídico alguno* .

Pues bien, las excepciones previstas en los arts. 8 y 9 de la Directiva deben constar igualmente en forma explícita y se justifican sólo por Anecesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales@ (C.33).

Igualmente la Directiva autoriza a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas (C.34).

Así mismo, se justificará el tratamiento de datos personales, en los siguientes casos: a) por parte de las autoridades públicas con fines, establecidos en el Derecho Constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realice por motivos importantes de interés público (C.35); b) en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados Miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas (C.36); y c) para el tratamiento de datos personales con *fines periodísticos o de expresión artística o literaria*, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias *a posteriori* como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales (art. 9 y C.37).

g) El *Principio de la información del interesado o titular de los datos.* Capital importancia adquiere el derecho a la información en el proceso informatizado de datos, pues es aplicable a todo el tratamiento, y por consiguiente,

a la fase de recolección de datos. Este derecho-principio de la información en la Directiva tiene especial regula-

ción teniendo en cuenta, sí la información en el marco de esta *sociedad de la información* [268bis], se ejercita en el caso de obtención de datos recabados del propio interesado (art.10), o sí se trata de la información cuando los datos no han sido recolectados del propio interesado (art. 11) [269], pues en uno y otro caso, se arbitran peculiares garantías y derechos para el titular de los datos (v.gr. *habeas data* y sus derechos estructurales: acceso, rectificación, actualización y cancelación de datos, así

(268 bis) La información el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos (C.14), así como a cualquier información que se considere de la persona humana y sea tratada mediante procesos informáticos, electrónicos o telemáticos. Texto completo en la dirección electrónica: WWW. CC.CEC (DATABASE CELEX).

(269) Este punto se considera significativo al ser incluido como uno de los aspectos de interés incluidos en el Anteproyecto de reforma a la LORTAD, tras la transposición de la Directiva 95/46/CE, al ordenamiento jurídico español, que debe acaecer el 31 de Octubre de 1998. Vid. GUTIERREZ SANCHEZ, Pedro. *ANTEPROYECTO DE LA LEY ORGANICA POR LA QUE SE MODIFICA*... Ob. cit., ut supra., pág.5.

como sus excepciones y limitaciones a los mismos [270] y el derecho de oposición al tratamiento, previstos en los arts. 12 a 15, respectivamente de la Directiva); así como, las obligaciones y derechos para los sujetos involucrados en el tratamiento de datos, particularmente del responsable o encargado del tratamiento.

En el primer caso, es decir, cuando los datos personales sean recolectados del propio interesado, la Directiva suministra unas pautas mínimas que deben cumplir los sujetos involucrados en el tratamiento, pero particularmente el responsable del tratamiento o su representante, quienes deberán comunicar a la persona de quien se recaben los datos que le conciernen, por lo menos la siguiente información, salvo que ya hubiera sido informado de ello (más no, que no se dé por informado, por otros medios):

a) La identidad del responsable del tratamiento y, en su caso, de su representante; b) Los fines del tratamiento de que van a ser objeto los datos; c) Información acerca de

---

(270) La Directiva en el art. 12, estatuye los derechos estructurales del ejercicio del derecho de habeas data, tales como el derecho de acceso, rectificación, actualización y cancelación de datos personales que resultaren inexactos o imcompletos. Así como las acciones informáticas de supresión y bloqueo de datos. *DERECHO DE ACCESO*: Los Estados Miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: 1. La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refirieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; 2. La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; y 3. El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las denominadas decisiones individuales automatizadas (art. 15-1); b) En su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se haya comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el literal b, si no resulta imposible o supone un esfuerzo desproporcionado. Art. 13. *EXCEPCIONES Y LIMITACIONES*: 1.- Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el art. 6-1 (relativos a los principios de la calidad de los datos), art. 10 (Información en caso de obtención de datos recabados del propio interesado), art. 11-1 (Información cuando los datos no han sido recabados del propio interesado), y los arts. 12 (Derecho de Acceso) y 21 (Publicidad de los tratamientos), cuando tal medida constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) interés económico y financiero importante de un Estado miembro o de la Unión Europea (UE), incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia los literales c, d, y e.,; g) la protección del interesado o de los derechos y libertades de otros derechos. 2.- Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados con medidas o decisiones relativas a personas concretas, los Estados miembros, podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el art. 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas@ Texto Completo de la Directiva 95/46/CE, en *WWW. CC.CEC* (Database Celex).

los destinatarios o las categorías de destinatarios de los datos; el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada un negativa a responder; y la existencia de derecho de acceso y rectificación de los datos que le conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Se puede apreciar, como lo sostienen *Doumortier y Alonso* **[271]**, la Directiva resulta en este aspecto nada formalista respecto del cumplimiento del deber de suministrar información al interesado, pues contiene una serie de elementos que

garantizan una mayor flexibilidad, pues p.e., considera no necesario informar al interesado cuando él ya dispone de la información pertinente, no se requiere informar sobre la identidad del encargado del tratamiento. En fin, el régimen de información al interesado, es mucho menos costoso y complicado que el de la Ley Belga sobre tratamiento informatizado de datos, que obligaba a informar aún en los casos ahora exceptuados de la Directiva.

En el segundo caso, es decir, cuando la información de los datos no han sido recolectados del propio interesado, aunque se aplica, a partir de la fase de registro de datos, previo almacenamiento de los mismos, por circunstancias temáticas la incluimos en esta fase inicial de recolección de los datos y haremos referencia puntal en los siguientes fases del proceso informatizado.

En desarrollo, de esta especial información cuando los datos no se recaben del interesado, el responsable del tratamiento o su responsable deberán, desde el momento del registro de los datos o, en caso de que piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la siguiente información, salvo si el interesado ya hubiere sido informado:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

---

(271) DUMORTIER Y ALONSO BLAS, D. Ob. cit., pág. 11.

b) los fines del tratamiento de que van a ser objeto de los datos; c) Información acerca de: 1. Las categorías de los datos de que se trate. 2. Los destinatarios o las categorías de destinatarios de los datos. 3. La existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se haya obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos legal respecto del interesado.

Se inaplicarán las anteriores informaciones, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En estos casos, estatuye la Directiva 95/46/CE, art. 11-2 *in fine,* que los Estados miembros establecerán Alas garantías apropiadas@.

h) El principio del derecho de oposición del interesado al tratamiento de datos, constituye una garantía de protección máxima de los derechos y libertades fundamentales en manos del interesado cuando dichos datos personales han sido sometidos a tratamiento (informatizado o no). Este nuevo derecho de los titulares de datos (C.25 y 30., conc., art. 14 y 15 Directiva), junto con el ejercicio del derecho *de habeas data* (acceso, rectificación y cancelación), constituyen la plataforma de defensa y protección que tiene toda persona dentro de la visión iusinformática de los derechos y libertades fundamentales, vale decir, de aquella parte de éstos y aquéllas en los cuales tiene incidencia los tratamientos y/o procesos informatizados en su pleno ejercicio, defensa y protección.

El derecho de oposición al tratamiento de datos, se manifiesta de dos formas: a) Como derecho de oposición al tratamiento propiamente dicho (art. 14); y, b) Como derecho de una persona a no verse sometido a una decisión individual informatizada con efectos jurídicos sobre aquella (art. 15).

El derecho de oposición del interesado, se ejercita por el interesado en cualquier momento del tratamiento de datos y Apor razones legítimas propias de su situación particular@ (o motivos fundados y legítimos relativos a su situación concreta. C.45), frente al tratamiento de cualquier dato personal que le concierna.

Ahora bien, se ejercitará este derecho de oposición en éstas condiciones por el interesado cuando: a) el tratamiento se requiere para el cumplimiento de una

misión de interés público o inherente al ejercicio del poder público conferido al responsable o a un tercero a quien se comuniquen los datos; y , b) Cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran su protección. En caso de oposición injustificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos.

El titular de los datos, también podrá ejercitar el derecho de oposición, previa petición y sin gatos, al tratamiento de datos personales que le conciernen en los cuales el responsable prevea un tratamiento destinado a la prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, p.e., de carácter político. Caso, contrario, podrá solicitar se informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

El derecho del concernido de datos personales a verse sometido a una decisión con efectos jurídicos (art.15 Ibídem), consiste en que las personas no podrán verse sometidas a una decisión individual informatizada que tiene efectos jurídicos sobre aquélla, o cuando les afecte significativamente y se basa únicamente en un tratamiento informatizado destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

Sin embargo, el concernido puede verse sometido a una decisión individual informatizada, en los siguientes casos: a) Cuando se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; y, b) Cuando esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Es claro, como sostienen *Dumortier y Alonso Blas* [272], que la efectividad del derecho de oposición (en sus dos vertientes, agregamos) exige que se concrete un procedimiento de tutela del mismo, así como la inclusión de la tipificación de las conductas que le son contrarias y la correspondiente sanción.

4.5.1.2.3. FASES DE ALMACENAMIENTO, REGISTRO Y CONSERVACION DE DATOS.

Sea lo primero, insistir que algunos de los principios comentados para la fase inicial de recolección de datos son de aplicación a todo proceso informatizado de datos, y como tal, aplicables a las fases de almacenamiento, registro y conservación de datos. Estos son: a) El principio de lealtad y licitud de los datos; b) El principio de veracidad y exactitud de los datos; c) El principio de legitimidad del tratamiento de datos, que a su vez se compone de los principios del consentimiento del titular, finalidad de los datos y prevalencia de ciertos intereses públicos y privados; d) El principio de interdicción de tratamiento de datos personales pertenecientes a las ACategorías Especiales; e) Principio de información del interesado o titular de los datos; y e) El principio del derecho de oposición del interesado al tratamiento informatizado de datos.

En efecto, estos principios aplicables a todo el tratamiento, en el contexto de la Directiva se observa el énfasis que se pone a *la fase de registro de los datos,* quizá porque es a partir de ésta, donde se presenta esa visión paradójica del derecho-protegido y el derecho-vulnerado, devenida con, por y para la estructuración de un procedimiento informatizado de datos personales, por parte de los sujetos que intervienen en el tratamiento informatizado de datos (interesado, titulares de datos, terceros, responsables

---

(272) Ibídem., pág. 6

y encargados del tratamiento, etc); así como por la importancia, en el marco actual de la Asociedad de la información@, a partir de la cual y tras el desarrollo de las nuevas tecnologías de la comunicación y la información (TIC), unidas a la informática, se pueden captar, transmitir, manejar, registrar, conservar y comunicar datos personales textuales, auditivos o sónicos o de imagen. Igualmente, porque día a día se van incrementando la formas de recolección de datos no directamente del interesado y se hace necesario establecer mecanismos de defensa, control y protección que garanticen al titular de esos datos una información precisa, clara e inequívoca (art.11), Adesde el momento mismo del registro de los datos, o a más tardar, al comunicar los datos por primera vez a un tercero@ (C.39 *in fine*), salvo que el interesado ya esté informado o Ala comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos@ (C.40).

Como principios específico de la fase de registro, es *el principio de publicidad de los tratamientos.* En efecto, si los procedimientos de notificación previos al tratamiento de datos (art.18 Id.) a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva (C.48), la publicidad de los tratamientos constituye una pieza importante para ejercitar los derechos y cumplir los deberes quienes están involucrados en el susodicho tratamiento, así como para que Acualquier persona@ pueda consultarlo, o para que se establezcan limites, restricciones o excepciones, según la categoría de los datos personales que se someten al tratamiento (art.21 Id.).

En *la fase de conservación de datos,* procede también, el *principio de identificabilidad de los interesados y de temporalidad de los datos*. En tal virtud, los datos personales se conservarán en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que

fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos (art.6 Id.).

4.5.1.2.4. FASE DE COMUNICACION DE DATOS: FLUJO O TRANSFERENCIA DE DATOS.

Como principios específicos para ésta fase, además de los principios generales del tratamiento de datos antes comentados en las otras etapas, podemos destacar el principio de confidencialidad y de seguridad del tratamiento y el de *la libre circulación de los datos* [273], los cuales guardan íntima relación cuando se somete a la fase de comunicación (por transmisión, cesión, difusión, etc) los datos personales previamente recolectados, almacenados, registrados y conservados. Cierto es que el principio de confidencialidad o secreto, como el de seguridad (técnica y jurídica) de datos se aplica a todas las fases del procedimiento, no es menos cierto que dicho principio se hace efectivo con mayor incidencia en la presente fase. Por esta razón, hemos incluido en este aparte su estudio.

El *Principio de confidencialidad y de seguridad del tratamiento.* Existe confidencialidad del tratamiento, cuando las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo pueden someter a tratamiento los datos a los cuales tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Por *el principio de seguridad del tratamiento*, el responsable del tratamiento está
obligado a aplicar las medidas técnicas (en consideración a los conocimientos técnicos

---

(273) Este capital principio aplicable en forma exclusiva a la fase de comunicación (por transmisión: emisión/ recepción) de datos personales, es uno de los principales objetivos de la Directiva

95/46/CE., cuando expresa: ALos Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada de los derechos y libertades fundamentales de las personas físicas, y en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales@ (art. 1). Más aún, Aa causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la Directiva 95/46/Ce, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad@ (C.9).Texto Completo de la Directiva en *WWW.CC.CEC* (Database CELEX).

y el coste de aplicación) y de organización adecuadas (es decir, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y la naturaleza de los datos por proteger), para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizado, *en particular cuando el tratamiento incluya la transmisión de datos de una red*, y contra cualquier otro tratamiento ilícito de datos personales (art.17-1 Id.).

El *principio de la libre circulación de datos*, desde la Recomendación de la OCDE de 1980, luego corroborada por el Convenio Europeo de 1981, ha constituido el eje central de la transmisión (emisión/recepción) de datos personales, a través de medios informáticos, electrónicos o telemáticos, porque se erige como el punto de equilibrio entre la protección de los derechos y libertades fundamentales de la persona humana y la liberación de obstáculos (técnicos y jurídicos) [274] para transferir datos entre los Estados miembros de la UE, o dentro del territorio de cada Estado entre organismos, personas jurídicas o físicas, públicas o privadas, sin que se eludan los mecanismos de seguridad, confidencialidad y protección de los datos, y a la vez, sin que representen un potencial riesgo a la vulneración de derechos y libertades fundamentales de la persona.

La Directiva 95/46/CE, con base en las normas comunitarias que le anteceden sobre la materia, regula en el Cap. IV, lo atinente a la ATransferencia de datos personales a países terceros@, reduciendo así el ámbito territorial de las

transferencias o flujos de datos a los estrictamente Ainternacionales@, cuando se refiere a la transferencia entre países miembros o no de la Unión Europea (UE), siempre y cuando se reúnan unos requisitos de forma y de fondo.

Las transferencias o flujos transfronterizos de datos personales son necesarios,

---

(274) A Para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados Miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones@ (C.8). Texto Completo de la Directiva en *WWW.CC.CEC* (Database CELEX).

principalmente según el C.56, para el desarrollo del comercio internacional, en tal virtud, las normas establecidas en la Directiva que prevalentemente se dirigen a la protección de las personas no se opone a la transferencia de datos personales a terceros países, siempre que garanticen un nivel de protección adecuado. El carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias.

La evaluación del nivel adecuado de protección garantizado por un país tercero, incluirá, entre otros aspectos: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países (art.25-2 Id.). Los Estados Miembros y La Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado. Una vez sea comprobado por la Comisión la falta de garantías por un país tercero, previo procedimiento establecido en la Directiva solicitará a los Estados que tomen las medidas necesarias para Aimpedir cualquier transferencia de datos personales@ con dicho país.

Sin embargo, podrá realizarse transferencia de datos con terceros países que no garantizan un nivel de protección adecuado, siempre y cuando se reúnan los siguientes requisitos: a) el interesado haya dado su consentimiento inequívocamente; b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, f) la transferencia tenga lugar desde un registro público, en virtud de disposiciones legales o reglamentarias, esté concebida para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta (art. 26-1).

También se podrá transferir datos personales a Aun tercer país que no garantice un nivel de protección adecuado..., cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas@ (art. 26-2).

Los Estados miembros de la UE, tienen la obligación de informar la aplicabilidad de las anteriores excepciones sobre transferencias de datos personales, a la Comisión, la cual a su vez, adoptará las medidas adecuadas, a través de un procedimiento administrativo sumarísimo previsto en el art. 31 de la Directiva.

De esta forma, como lo sostiene *Dumortier y Alonso Blas* [275], la Directiva establece reglas claras con respecto a las transferencias internacionales de datos: total libertad dentro de la Comunidad y prohibición (con excepciones), cuando se trate de países terceros que no garanticen un nivel adecuado de protección.

4.5.2. LA DIRECTIVA 97/66/CE*, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI)* [276] *y las redes móviles digitales públicas.*

La fase informatizada de comunicaciones (o Atelecomunicaciones@ como prefiere, la Directiva) de datos personales con el desarrollo constante y revolucionario de

---

(275) DUMORTIER Y ALONSO BLAS, D. Ob. cit., pág. 11.

(276) El Parlamento ha subrayado la importancia de proteger los datos personales y la intimidad en las redes de telecomunicaciones, especialmente en relación con la introducción de la Red Digital de Servicios Integra- dos (RDSI). El Consejo de la UE, en la Resolución de 18 de Julio de 1989, ya había hecho énfasis en la mencionada protección y sobre una mayor coordinación estatal sobre el tema de la RDSI. En la Parte IV. Punto 5 y ss., haremos comentarios puntuales sobre el tema

las nuevas tecnologías de la información y comunicación (TIC) [277], día a día, se va super especializando cara a los intereses, derechos y libertades fundamentales dignos de protección y garantía por parte del Estado e incluso de los mismos particulares; así como el de preservar los principios de *la libre circulación de los datos* y la confidencialidad de las comunicaciones [228] que transiten entre los Estados de la UE, conjuntamente con los cada vez, paradójicamente por el mismo avance, espectros de riesgo y vulnerabilidad que crecen geométricamente y se concretan; entre otras actividades, en el acceso, la transformación o la interceptación no autorizada de datos personales y continentes en bases de datos públicas o privadas, a través de medios muy sofisticados de tipo informático, electrónico o telemático. Acciones humanas indebidas, abusivas o ilegales que generan reproche social y normativo que en España van, desde las sanciones administrativas por infracciones (o contravenciones) al régimen del tratamiento informatizado de datos personales, previsto en la LORTAD, hasta las sanciones

penales por estar incursos en formas delictuales contra los derechos y libertades fundamentales (entre ellos, la intimidad, la imagen y el honor, la información, etc.) [279].

La Directiva 97/66/CE, constituye una norma jurídica comunitaria que refuerza,

---

(277) En efecto, son los Estados de la UE, quienes mediante sus disposiciones normativas, garanticen, la con- fidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicaciones y de los servicios públicos de telecomunicaciones. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente (C.5).

(278) El Parlamento Europeo y el Consejo de la Unión Europea (UE), consciente de dichos avances y de que la Directiva 95/46/CE, constituye un buen instrumento, pero jamás suficiente, de defensa de los derechos y libertades fundamentales de la persona humana, ha venido trabajando una propuesta común que se concre-te en una Directiva Comunitaria que refuerce y especialice la protección de esos intereses y derechos, ya que Aen la actualidad están apareciendo en la UE nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios; que el desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de telecomunicaciones; que el desarrollo transfronterizo de estos servicios, como el vídeo por pedido o la televisión interactiva, depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad@ (C. 2). Texto Completo de la Proposición Común (CE) No. 57/96, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales, en WWW. *CC. CEC (Database CELEX).*

(279) En la Parte IV, hablaremos sobre estos temas. Así mismo plantearemos a título de ensayo el delito que llamamos de *datos personales registrados en forma automatizada contra la intimidad*. Este consta de dos partes: una, configurada por el acceso, utilización y alteración de los datos (parte *ab initio del tipo*); y otra, estructurada por la interceptación o intervención de los datos, por medios informáticos, electrónicos o telemáticos (parte *in fine del tipo*). Todo ello, con base en el estudio y análisis del actual Código Penal (Libro II, Delitos y Penas: Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio) y las normas extrapenales como la LORTAD y las Directivas 95/46/CE y 97/66/CE, sobre telecomunicaciones e intimidad.

amplía y concreta el régimen previsto en la Directiva 95/46/CE, sobre protección a los derechos y libertades fundamentales (particularmente, el derecho a la intimidad) de las personas humanas, cuando sus datos han sido tratados con medios informáticos, electrónicos o telemáticos, haciendo énfasis en la fase de transmisión (emisión/recepción) de datos. En tal virtud las normas de la Directiva 95/46/CE, se aplicarán por extensión, en cuanto a los recursos judiciales, régimen de responsabilidad y sanciones (art. 14-2); así mismo se podrá limitar el alcance de las obligaciones y derechos previstos en los denominados por la Directiva 95, APrincipios relativos a la calidad de datos@ (art.5 y 6), y los datos de Acategorías especiales de tratamiento@ (art. 8-1 a 8-4), cuando dichas limitaciones constituyan

una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicaciones (art. 14-1).

La Directiva consta de una parte interpretativa y hermenéutica (26 considerandos) y un cuerpo normativo, con los siguientes temas: Objetivo y ámbito de aplicación (art. 1), Definiciones (art. 2), Servicios regulados (art.3), Seguridad (art.4), Confidencialidad de las comunicaciones (art. 5), Tráfico y facturación (art.6), Facturación desglosada (art. 7), Presentación y limitación de la identificación de la línea llamante y conectada (art. 8), Excepciones (art. 9), Desvío automático de llamadas (art.10), Guías (11), llamada no solicitada (art. 12), Características técnicas y normalización (art. 13), Extensión del ámbito de aplicación de determinadas disposiciones de la Directiva 95/46/CE (art. 14), Aplicación de la Directiva (art.15), y Destinatarios (art. 16).

4.6. AUSTRALIA: LEY DE LA INTIMIDAD Y LA PROTECCION DE LOS DATOS: BILL AUSTRALIANA DE 1994.

The Privacy and Data Protection Bill 1994 (NSW), [280] es una de los más recientes Estatutos normativos de corte anglosajón que regulan la protección de los

---

(280) Texto original y completo en inglés en : WWW. AUTLI. EDU. AU. (Database de la Universidad de Australia).

derechos fundamentales de la persona humana, especialmente el derecho a la intimidad, cuando los datos personales han sido sometidos a un proceso informatizado, con medios informáticos, electrónicos o telemáticos.

La Ley de 1994, esta estructurada en cinco (5) partes y cuatro (4) cláusulas finales remisorias a otras leyes aplicables subsidiariamente a ésta, tales como la Ley de la Intimidad Australiana de 1988 (*Privacy Bill 1988*); entre otros temas, sobre el AComisionado para la protección de la Intimidad@ (*Privacy Commissioner*), el

Consejo Consultivo de la protección de la Intimidad (Privacy Advisoy Committee) , la regulación de la libertad de información (*Freedom of information Act 1989*) [281] y la Ley de regulación del Defensor del Pueblo (*L´Ombusdman Act 1974*). Cada parte, a su vez, contiene divisiones, secciones y artículos.

LA PARTE PRIMERA. PRELIMINARES.

En esta parte se hace referencia; entre otros, a los siguientes temas:

1. *OBJETIVOS DE LA BILL AUSTRALIANA DE 1994.* Los cuales se resumen así: a) Estatuir los mecanismos de protección de los titulares de los datos personales en las diferentes fases del tratamiento informatizado, y sobre todo, en la etapa de recolección, como en la posterior utilización, consulta, divulgación o descubrimiento de dicha información personal, tanto realizadas por las autoridades Estatales, como por personas u organismos del sector privado, b) Atribuir funciones específicas a la oficina del Comisionado para la protección del derecho a la Intimidad, sobre éstas materias, c) Organizar el Comité Asesor para la protección de la Intimidad; d) Derogar las normas contrarias, en especial, las referidas al Comité Asesor previstas en la ABill@ de 1975.

. 2. DEFINICIONES TECNICO-JURIDICAS. Contiene un amplio glosario de términos jurídicos y técnicos (iusinformáticos) utilizados en todo el texto normativo de

---

(281) Según el art. 51 de la Bill 1994, no será objeto de requerimiento o descubrimiento de información, aquellos conceptos y disposiciones que regulan la información general e incluso personal que no afecta la intimidad ni los datos personales informatizados y previstos en La Ley de protección a la información Australiana de 1989.

la Bill 1994. Entre otros, destacamos los siguientes:

a) *Recolector de datos* (ACollector@). Personas, autoridades u organismos con funciones públicas o privadas, o en su caso, sus representantes, dedicados a la

colecta de información de carácter personal. Estas funciones incluyen derechos, deberes y obligaciones para quienes las ostentan.

b) Jefe de una Autoridad Pública. Se utiliza para referirse a los Jefes de una oficina administrativa, Autoridad Gubernamental local, Directores del Servicio de Educación, Servicio de Policía, etc.

c) *Información personal*. Cualquier información u opinión sobre una persona, incluida la que hace parte de un banco de datos, sea verdadera o no, bien sea almacenada en forma material o con medios informáticos. La información personal identificará a una persona o permitirá razonablemente identificarla.

d) *El Comsionado para la protección de la Intimidad* . Es la autoridad encargada de salvaguardar, proteger y hacer cumplir las normas sobre la protección del derecho a la intimidad cuando se sometan a tratamiento informatizado los datos personales.

e) *Registro Público*. Es el asiento o registro de una información personal ante las personas o autoridades competentes, cuando la ley así lo requiere, para publicitarla, ponerla a disposición o consulta de aquellos que están habitados por la ley para hacerlo.

f) *Unidad de información personal informatizada* (ARecord@). Esta unidad, puede esta contenida, a los efectos de la Bill 1994, en: 1. Documentos. Incluye además de los tradicionales documentos, los definidos como tales, en la *Act 1987* v.gr. Los discos informáticos, cintas u otros artículos que pueden almacenar o grabar sonido, imágenes o mensajes capaces de ser reproducidos por emisión o recepción; b) La información contenida en una fotografía o representación pictórica de una persona, pero no incluye la que se halle en una revista, libro, periódico u otra publicación que son o están, por regla general, a disposición del público, o aquellas imágenes de una persona que se hallan en los Archivos del Estado (AState Archive@.

Previstos en The Archives Act 1960), tales como en Bibliotecas, Galerías de Arte o Museo y en los cuales se tiene el propósito referenciales o de investigación, como para el estudio, la realización de escritos o artículos, para la exhibición, o finalmente para la transmisión electrónica o por cable teniendo en cuenta los anteriores fines.

g) *Vigilante de los datos o Informaciones Personales* (ARecord-Keeper@). Es la persona u organismo responsable de la posesión y administración de una información personal. El vigilante de los datos, también se le conoce como Vigilante o responsable de los registros. Este puede ser público o privado, según la información personal que posea o administre.

PARTE II. VIGILANCIA Y PROTECCION DE LOS DATOS O INFORMACIONES PERSONALES.

Esta parte se subdivide en cuatro (4) divisiones, que tratan a su vez, los temas siguientes: a) Tratamiento de información en el Sector Público; b) Los Códigos de Protección de los Datos personales (*Data protection Codes*: En el Sector Público [282]

---

(282) La Bill Australiana de 1994 en la División II, artículos 10 a 12 se refiere a estos temas. ADivision 2. Data protection codes. SECT 10. Data protection codes must be prepared for public sector. 10. (1) For the purpo-se of better protecting individual privacy, a data protection code relating to the collection, use and disclosure, and procedures for dealing with, personal information held by a public authority must be prepared y Th heda of Th publica adherida ad adoptad y Th publaca adhegida. (2) Th conde mus be preparado ad adoptad no later Th 12 montas afer Th commencement of this section or the establishment of the authority, whichever is the later. (3) This section applies to personal information about any persons, including the employees of public authorities. SECT 11. Requirements for public sector data protection codes. 11. (1) A data protection code of a public authority must: (a) specify procedures for dealing with personal information; and (b) specify conditions to be imposed as to the disclosure by the Archives Authority of New South Wales of public records (within the meaning of the Archives Act 1960) that are records of the public authority or information contained in them; and (c) be submitted to the Privacy Commissioner for review before adoption. (2) The code must, in relation to procedures for dealing with personal information, conform, so far as is reasonably practicable, to the data protection principles set out in Division 4. (3) That part of the code relating to conditions to be imposed on the Archives Authority of New South Wales must conform, so far as is reasonably practicable, to Principle 10 of the data protection principles. (4) Despite subsections (2) and (3), a code may permit personal information to be disclosed by the public authority to another public authority for the purposes, and in the circumstances, specified in the code. (5) Before a code is adopted, the head of the public authority must consider the findings of the

review of the code by the Privacy Commissioner. SECT 12.Amendment of public sector data protection codes. 12. (1) The head of a public authority may, from time to time, amend its data protection code and must submit the amendment to the Privacy Commissioner for review before adoption. (2) Before the amendment is adopted, the head of the public authority must consider the findings of the review of the amendment by the Privacy Commissioner@. Texto completo en: *WWW.AUSTLI. EDU.CO*. (Database de la Univ. De Australia).

y en el Sector Privado [**283**]); c) Los Registros Públicos; y d) Los principios de Protección de los datos personales.

Los principios de protección de los datos aplicados a las diferentes fases del procedimiento informatizado en la *Bill 1994* de Australia, están previstos en el artículo 21 de la siguiente forma:

1. *Principio de finalidad en la recolección de los datos*. Los datos personales deberán ser recolectados por las personas u organismos (públicos o privados) para los fines o propósitos previstos en las leyes y directamente relacionados con sus funciones o actividades. La información personal, por tanto, para cumplir estos fines y propósitos no será recogida por medios ilegales o injustos.

2. *Principio de información de los datos personales al concernido*. El interesado podrá solicitar directamente la información de los datos personales que le conciernen, a quienes la han recogido (Colectores), excepto si autoriza a otra persona para que descubra o divulga la información de conformidad con los principios de la *Bill 1994*

---

(283) Códigos de protección de datos en el Sector Privado: ASECT 13. Private sector data protection codes. 13. (1) The Privacy Commissioner may, at the request of a person or body that is not a public authority, prepare a data protection code relating to the collection, use and disclosure, and procedures for dealing with, personal information held by the person or body for adoption by the person or body. (2) A person or body that is not a public authority may prepare and adopt a data protection code relating to the collection, use and disclosure, and procedures for dealing with, personal information held by the person or body and may submit the code to the Privacy Commissioner for review. SECT 14. Requirements for preparation of private sector data protection codes. 14. (1) In preparing a data protection code under this Division for a person or body that is not a public authority, the Privacy Commissioner must specify procedures for dealing with personal information. (2) The code must conform, so far as is reasonably practicable, to the data protection principles set out in Division 4. SECT 15.Amendment of private sector data protection codes. 15. (1) A person or body that is not a public authority may, from time to time, amend its data protection code and must submit the amendment to the Privacy Commissioner for review before adoption. (2) Before the amendment is adopted, the person or body must consider the findings of the review of the amendment by the Privacy Commissioner. SECT 16.Exemptions from

public and private sector data protection codes. 16. (1) The Privacy Commissioner may, at the request of the head of the public authority or other person or body by or for whom a data protection code is or is to be prepared, exempt personal information or classes of personal information or a person or any classes of persons from any or all of the provisions of the code. (2) A data protection code must identify any personal information or persons or classes of personal information or persons exempted from any or all of the provisions of the code. (3) An exemption may be revoked or varied at any time by the Privacy Commissioner on request by the head of a public authority or other person or body by or for whom a data protection code is or is to be prepared. (4) An exemption in a data protection code of a public authority may be revoked or varied at any time by the Privacy Commissioner on the Commissioner's own initiative. (5) The Privacy Commissioner is to review each exemption given by the Commissioner if it is still in force 3 years from the date it is given or was last reviewed. The review is to be undertaken as soon as possible after the end of the period of 3 years from that date@. Texto completo en: *WWW.AUSTLI. EDU.CO*. (Database de la Univ. de Australia).

de Australia y siempre y cuando sea utilizada para ser incluida en un registro o una publicación disponible o accesible al público y se tomen por parte del Recolector todas las medidas de seguridad seguidas en la recolección, y siempre y cuando sea informado previamente al concernido, si fuere posible, sobre los siguientes aspectos: 1) Propósitos de la recolección; 2) Sí ha sido autorizada por la ley; 3) La naturaleza obligatoria o voluntaria de la recogida de datos; 4) Los efectos en el concernido al proporcionar parte o toda la información solicitada; 5) La existencia de los derecho de acceso y rectificación de los datos (*habeas data*), y si fuere el caso, la cancelación; 6) El nombre y dirección del Vigilante y Protector de los datos; y, 7) Cualquier otra información sobre las personas, organismos o agencias que tengan actividades de recolección de información personal y estén relacionadas con sus datos personales.

3. *Principio de solicitud de información disponible o de acceso al público.* Los datos personales recogidos en un registro o disponibles en una publicación de acceso al público, pueden ser solicitadas por el recolector de los mismos, siempre que la información sea pertinente, no exceda los propósitos para los cuales fue recabada, sea exacta, completa y actualizada. Igualmente que la información no constituye un obstáculo irrazonable en los asuntos de la persona concernida

4. *Principio de almacenamiento y seguridad de la información*. El vigilante del registro de los datos personales ejercerá el control de los mismos. En virtud, los datos serán protegidos para que: a) sean posteriormente utilizados con los mismos propósitos explícitos y legales para los que fueron almacenados; b) Sean igualmente utilizados en forma adecuada, pertinente y en forma no excesiva respecto de los

propósitos con los que se recabaron; c) Sean procesados o tratados justa y legalmente; d) Sean almacenados
por un espacio de tiempo necesario concordante con los fines y propósitos de dicho almacenamiento; e) la protección del almacenamiento se extienda a las medidas de seguridad necesarias contra el adquisición, la pérdida, el acceso desautorizado, uso, modificación, descubrimiento o divulgación, y contra cualquier otro mal uso de datos; y, f) Si fuese necesario, para evitar un uso desautorizado o descubrimiento de datos, será implementado un servicio especial de vigilancia y protección de datos, según lo considere razonable el Vigilante del Registro de datos.

5. *Principio de información relacionada con los datos personales registrados por el Vigilante de los mismos.* El vigilante podrá informar a cualquier persona cuando se lo solicite acerca de la existencia de la posesión y control de cualquier dato personal que le concierna y si existe algún otro dato adicional que se relacione con el solicitante. En tal virtud, le informará sobre: a) la naturaleza de la información; b) los propósitos principales para los cuales será utilizada la información; c) los trámites que debe seguir para hacer uso y ejercicio del derecho de acceso a los datos personales o registros.

Sin embargo, el Vigilante de los datos, podrá negarse a suministrar información en las condiciones anteriormente descritas, si el solicitante no está autorizado por la ley o documento.

El Vigilante de los datos personales, deberá mantener y poder informar de: a) la naturaleza de los datos personales; b) las fuentes de información que suministraron los datos; c) los propósitos para los que fueron recaudados los datos, así como la autoridad que tiene su posesión y control; d) el propósito específico de almacenamiento de cada dato personal; e) las clases de personas acerca de las cuales se almacena un dato; f) el período de tiempo por el que se almacena un dato; g) las personas que son titulares para ejercer el derecho de acceso a la información personal y las condiciones bajo las cuales ostentan dicha titularidad; h) los trámites

que deben seguir los titulares de los datos para ejercer el derecho de acceso a los datos que les conciernen.

El Vigilante de los datos mantendrá un registro de los anteriores datos, a fin de ponerlos a disposición de inspecciones realizadas por autoridades (administrativas o judiciales), cuando así se lo requieran o por disposición legal. Así mismo, para enviar una copia en el mes de junio de cada año, con destino al Comisionado de Protección para la Intimidad.

6. *Principio de Acceso a los datos personales registrados por el concernido*. El Vigilante de los datos, permitirá el acceso a los datos personales que le conciernen, sin demora y sin gasto alguno. El acceso no se permitirá a la totalidad de los registros o informaciones almacenadas y registradas, si no es con autorización legal o documento que así lo acredite.

7. *Principio de alteración de los datos personales.* El Vigilante de los datos, podrá proceder a las correcciones apropiadas, cancelaciones y modificaciones a los datos en circunstancias legales y que aseguren la integridad de los datos, siempre que el dato no sea exacto o completo o, no esté conforme a los propósitos para los cuales fue recabado y almacenado.

Si los datos personales han sido corregidos, anulados o agregados de conformidad con las razones y circunstancias anteriores, el titular de los datos o concernido será informado y notificado de dichas alteraciones. Sin embargo, este principio podrá ser limitado conforme a la aplicación de una ley estatal, cuando se trate del ejercicio de derechos contenidos en un documento que se requiera corregir o enmendar. Es el caso de los documentos en los cuales el Vigilante de los datos no esta legado para enmendarlo con correcciones, adiciones o cancelaciones, de conformidad con la petición (o demanda) de la persona concernida y las previsiones legales de la Bill 1994.

8. *Principio de Veracidad de la información personal antes de su utilización.* El Vigilante de los datos no permitirá el uso de los datos, sin previamente tomar las medidas necesarias para asegurar que la información personal está conforme a los propósitos para los cuales se solicita su utilización, así como que la información es pertinente, exacta, actualizada y completa.

9. *Principio de límites para el uso de la información personal (datos).* El Vigilante de los datos, no permitirá el uso de la información personal con propósitos diferentes para los cuales fue recabada y almacenada, salvo que: a) la persona concernida haya dado su consentimiento para el uso de conformidad con dicho propósito; b) el Vigilante de los datos presuma razonablemente que con la utilización de dicha información personal se puede prevenir o disminuir una amenaza seria e inminente a la vida o a la salud de individuo concernido u a otra persona; c) el uso de la información personal es necesaria para la investigación (judicial o policiva) de conformidad con la Ley Penal o Ley de Impuestos, o para la protección de un crédito público; d) el uso de la información personal sea requerida por autorización legal; y, e) el uso de la información personal está relacionado directamente con el propósito para el cual fue recabado.

10. *Principio de los límites al descubrimiento o divulgación de la información personal (datos).* El vigilante de los datos, no permitirá el descubrimiento de la información personal a una persona, organismo o agencia de recolección de datos, a menos que: a) la persona concernida haya estado informada previamente de dichos propósitos; b) la persona concernida haya dado su consentimiento al descubrimiento; c) el Vigilante de los datos presuma razonablemente que el descubrimiento de información personal es necesario para prevenir o disminuir una amenaza seria e inminente a la vida o a la salud de la persona concernida u a otra persona; d) el descubrimiento es requerido o autorizado mediante ley estatal; e) el descubrimiento es necesario para una investigación (administrativa o judicial), según la Ley Criminal o Ley de Impuestos, o para la protección de un crédito público.

El uso que se debe dar a la información personal descubierta en las circunstancias y condiciones anteriores será única y exclusivamente el que corresponda al propósito para el cual fue solicitado. En caso del descubrimiento para investigaciones se hará constar en una nota al margen el uso específico de la información personal.

11. *Principio de los límites en el uso de Ainformación personal sensible@ (ACertain Information* [284] @) . Muy a pesar de los dos principios anteriores (9 y 10), la información personal relacionada con el origen étnico o racial, las opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos o, los relativos a la salud o vida sexual, no podrán ser descubiertas por el Vigilante de los datos, sin el consentimiento expreso y escrito, libremente otorgado por la persona concernida, excepto si está autorizado por ley.

---

(284) La Bill 1994 de Australia, emplea la terminología de ACertain Información@ (información segura), para referirse a la información personal sensible o ADatos sensibles@.

La información personal relacionada con la historia delictiva de una persona, sólo podrá procederse a su descubrimiento, cuando sea requerida o por autorización legal o por la Bill 1994.

PARTE III. EL COMISIONADO PARA LA PROTECCION DE LA INTIMIDAD.

Contiene dos Divisiones: a) Sobre las quejas e investigaciones; y b) Los Informes.

Enunciaremos algunas de las funciones principales del Comisionado en relación con la protección de los datos del concernido, previstas en el art. 22 de la Bill 1994. Estas son: a) Promover la adopción de los principios de protección de los datos y las pautas para lograrlo con miras a promoción de la Intimidad tanto en el

sector público como en el sector privado, b) Dirigir las investigaciones en materia de protección de los datos y la intimidad de las personas, c) Proporcionar ayuda a las autoridades públicas que lo requieran sobre los *Códigos de Protección de los datos*, d) Suministrar consejos a cualquier persona acerca de la necesidad o conveniencia de implementar instrumentos legislativos, administrativos o de otra índole en interés de la intimidad de las personas, e) Supervisar los desarrollos tecnológicos TIC e informática e informar a los interesados para minimizarlos, si éstos pudieran tener un impacto adverso en la protección de los datos y a la intimidad, f) Recibir e investigar y, si fuese procedente, conciliar las quejas sobre el uso y descubrimiento de la información personal (pública o privada) o de otras vulneraciones a la intimidad, g) Redactar un informe Anual sobre las quejas y recomendaciones al Ministro. Así mismo, presentar un informe especial al Parlamento, cuando sea requerido por éste; y, h) Preparar y publicar un catálogo sobre los registros que llevan los Vigilantes de los datos, con la información relacionada en el principio 5, en particular sobre las autoridades públicas allí relacionadas.

PARTE IV. EL COMISIONADO PARA LA PROTECCION DE LA INTIMIDAD.

En esta parte de la *Bill 1994* de Australia, se hace referencia a las calidades requeridas para ser nombrado como Comisionado de la protección de la Intimidad, el personal adscrito a dicha dependencia, cuando se trate en el sector público, así como las funciones especiales y generales y los poderes de delegación para cumplimiento de las mismas, aprobadas por el Ministro correspondiente.

PARTE IV. EL COMITE ASESOR PARA LA PROTECCION A LA INTIMIDAD.

Hace referencia al Comité Asesor para la protección a la intimidad, designación de los miembros que lo componen y funciones. Su función prioritaria es aconsejar al Comisionado para la protección de la intimidad en las materias

relacionadas con sus funciones (tanto en el sector público como privado), así como recomendar puntualmente los aspectos (técnicos o jurídicos) para que sean incluidos por éste en la protección de los datos personales y la intimidad.

PARTE VI. DISPOSICIONES VARIAS. (A*Miscellaneous*@).

Contiene las disposiciones generales y funciones previas del Comisionado para la protección a la intimidad sobre el AProcedimiento de Contravenciones@ o de infracciones a la Bill 1994 (las cuales se relacionan taxativamente en el art. 49), tales como el envío de la información precisa para que sea adelantada una investigación por un A*Tribunal Local*@ (Local Court), así como la aplicación de las excepciones para descubrir información personal en estos casos.

ORDENAMIENTOS JURIDICOS DE PROTECCION Y GARANTIA DE LA VISION IUSINFORMATICA DE LA INTIMIDAD, A TRAVÉS DE LAS LEYES DE PROTECCION DE DATOS PERSONALES.

4.1. PRELIMINARES.

Nos parece oportuno en esta parte del trabajo, hacer mención a los diferentes cuerpos normativos que regulan el tratamiento informatizado de los datos de carácter personal, a efectos de exaltar, entre otros aspectos, por un lado, la labor que vienen cumpliendo los legisladores en los diferentes Estados del mundo por puntualizar y establecer un marco de garantías y medias de protección a los derechos involucrados en dicho tratamiento (derechos a la información, expresión, habeas data, honor, imagen, intimidad, etc); y por otro, analizar, estudiar y puntualizar la *visión iusinformática* del derecho a la intimidad, prevista en las principales leyes de protección de datos personales, clasificadas inicialmente en *tres generaciones*, según sus contenidos y evolución en la regulación del fenómeno informático en entronque con el derecho. Ampliaremos luego una cuarta generación y otra en transición, atendiendo además de lo dicho, al factor temporal, los avances significativos de iusinformática y la consideración de los Estados "paraísos informáticos" técnica como legislativamente.

En la *primera generación* de estas leyes se hallan las denominadas *leyes pioneras* en la regulación y tratamiento (informatizado o no) de datos de carácter personal: La *LEY FEDERAL ALEMANA DE PROTECCION DE DATOS PERSONALES* y Ley Sueca "*Data lag"* de 11 de mayo de 1973 [130] . Según *Mirabelli* [131] , estas leyes son tendencialmente restrictivas puesto que se sujetan al requisito de "la autorización previa" para la creación de los "*ficheros"* o bancos de datos, limitando excesivamente la recolección de los "datos sensibles" e instituyendo organismos con funciones y estructura cuasi jurisdiccional para la concesión y el ejercicio del control de

---

(130) La Data lag Sueca, según el profesor ORTI, "estableció un sistema de Registro de ficheros informatizados, exigiéndose la inscripción con carácter constitutivo, necesaria para obtener la autorización para crear un fi- chero, y a la que se condicionaba la inclusión en el Registro. Este requisito fue sustituido más tarde por el sistema de la mera notificación e inscripción registral, que es el seguido en la ley española" Cfr ORTI VALLEJO, Antonio. *DERECHO A LA INTIMIDAD E INFORMATICA (Tutela de la persona por el uso de ficheros y tratamiento informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*. Ed. Comares, Peligros (Granada), 1994, pág.14.

(131) MIRABELLI, "*Banche dati e contemperamento degli interessi", Bance dati telematica e diritti della persona*, Cedam, Padova, 1984, pág. 160. Citado por ORTI V. Ob. cit., pág. 11.

los mencionados banco de datos [132]. Sin embargo, como veremos más adelante la Ley Alemana, --que tomamos como prototipo de análisis de esta primera generación-- por contra, se caracteriza por ser la primera en el tratamiento integral de tratamiento informatizado o no de datos personales, así como de demarcar una nueva técnica legislativa en materia de definiciones técnico-jurídicas, estructurar por vez primera los "procesos de datos" públicos y privados y crear la figura del Comisario de Protección de datos para la vigilancia, garantía y protección de los derechos fundamentales, las libertades públicas e intereses legítimos de los titulares de datos personales. Temas que se tratarán brevemente, pues sirven a los propósitos iniciales y finales de la investigación.

En una *segunda generación de leyes* protectoras de los datos personales se destacan la de Francia en 1974, Noruega en 1978, Luxemburgo en 1981, etc. Por paralelo y con idénticos propósitos, surgen normas de ámbito internacional (La Recomendación de la OCDE de 1980) y Comunitario Europeo propuestas por el Consejo de Europa (El Convenio de Estrasburgo de 1981). Las leyes en esta etapa se caracterizan por el sistema de "la notificación" y no de la autorización como requisito *a priori* para crear bancos de datos. Además, se introduce la figura del responsable del fichero o banco de datos [133], se ingresa en la técnica legislativa de la conceptualización de los términos técnico cerrados y abiertos utilizados en las nuevas tecnologías de la información y la comunicación (TIC) que inciden en el derecho y se instituye, a partir de éstas, los denominados "principios fundamentales de la protección de datos", tanto en el tratamiento, almacenamiento, difusión como en la "libre circulación de datos de carácter personal". Aspectos capitales en el procedimiento informatizado de datos que se evidenciaron más en las normas de ámbito internacional y comunitario, antes que en las leyes estatales, como precisaremos.

Por ello, tomaremos de ésta generación dos prototipos de legislación sobre el tratamiento informatizado de datos: La Recomendación del Consejo de la OCDE de Septiembre 30 de 1980, *por la que se formulan directrices en relación con el flujo*

---

(132) En ésta etapa de clasificación de normas de protección de datos personales, nacieron por doquier varias leyes en Europa y América.. Se destacan entre ellas la Ley Francesa de 6 de Enero de 1978, conocida como "*Loi relative à l´informatique, aux fichiers et aux libertés,* y la *Privacy act* de 31 de diciembre de 1974, que

fueron el prototípo de otras que les siguieron . Entre ellas, la Ley Noruega de Junio 9 de 1978, la de Luxemburgo de 30 de Marzo de 1979, la Suiza de 1981.

(133) Ob. ut supra cit. pág. 11.

internacional de datos personales y la protección de la intimidad y las libertades fundamentales y El Convenio Europeo de Estrasburgo de 28 de Enero de 1981", relativo a la *"protección de las personas con respecto al tratamiento automatizado de datos de carácter personal"*. Convenio incorporado por todos los Estados Europeos en sus respectivos ordenamientos jurídicos internos a través de normas jurídicas de trasposición. En España, el Convenio se ratificó mediante instrumento de Enero 27 de 1984 (BOE. 15-11-1985, núm. 274) e ingresó al ordenamiento jurídico interno no sólo como mecanismo de interpretación de derechos humanos (art.10.2 CE), sino como una verdadera norma jurídica con fuerza legislativa desde aquélla época (art.96.1 CE).

En la *"tercera generación"*, se ubican las normas jurídicas nacidas en la década de los noventa, muy a pesar de que las propuestas e iniciativas venían manejándose desde la década anterior. En esta se ubican la *"La ley española de regulación del tratamiento automatizado de datos de carácter personal"*, de 29 de Octubre de 1992, conocida también como LORTAD, como también la *"Privacy and data Protection Bill 1994 (NSW) o Ley de protección de la intimidad y los datos personales en Australia.* Esta generación de leyes se caracteriza según *Orti Vallejo* [**134**], siguiendo a *Pérez Luño*, por ser más "liberalizantes del uso de ficheros de datos personales" y establecer un amplio marco de principios, derechos y obligaciones para las personas naturales, jurídicas, públicas y privadas.

Una *cuarta generación* de normas surge con la expedición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.* Esta generación se caracteriza por plantear como epicentro el principio-derecho de la libre circulación de datos personales

entre los países miembros de la Unión Europea e incluso entre países terceros, previo el lleno de unos requisitos *sine qua nom;* la consagración de principios, derechos (como el de información y de habeas data) y obligaciones en todas las fases, etapas o ciclos informáticos del procedimiento informatizado de datos, cuando se realiza con soportes, medios y aplicaciones informáticas, electrónicas y telemáticas [**135**] y la plasmación del llamado *derecho de oposición al tratamiento*

informatizado de datos personales, como un derecho personalísimo de los titulares de los datos personales.

---

(134) ORTI VALLEJO, A. Ob. cit.. pág. 18

Finalmente, una *quinta generación* o *generación de leyes protectoras de datos específicas en tránsito*, constituida por Estados que no disponen de normas especiales en la protección de datos personales, pero en cambio disponen de diversas normas jurídicas generales, mecanismos y procedimientos jurisdiccionales de índole constitu- cional, contencioso-administrativo, civil y penal. Igualmente, disponen de recursos en "vía administrativa" contra las decisiones, actos u operaciones del Estado y normas que regulan aspectos puntuales (v.gr.El derecho a la información, habeas data, etc), pero no integrales del tratamiento informatizado de datos personales. En todo caso, estos Estados con este conjunto de normas e instituciones jurídicas, propenden por la efectiva protección de los derechos y libertades fundamentales, en todos los ámbitos incluidos aquellos que se presentan en el tratamiento informatizado de datos. Quizá por ello, en puridad no existen "*Estados paraísos informáticos*"por el sólo hecho de no tener normas superespecíficas en algunas materias que develan la tensión-relación de la informática con los derechos humanos, pues estas están inmersas en una amplia gama de protección general de los derechos fundamentales que todo Estado dispone. En el derecho Colom- biano, se dispone de una regulación constitucional específica de los derechos fundamentales de la intimidad, del habeas data, del libre desarrollo de la personalidad, de la información y de expresión (arts.15, 16,20,73,74 Cons.Pol.), así como un ordenamiento jurídico que desarrolla el derecho de la información y el habeas data (Ley 57/1985, C.C.A de 1984/1989, etc) como mecanismos coadyuvantes de protección de los derechos fundamentales, entre ellos el de la intimidad, cuando se esta ante procedimientos de datos informatizados o no. Así mismo se cuenta con una amplia, fruc tífera y puntual jurisprudencia de la Corte Constitucional,"salvaguarda de la Constitu- ción", la cual va desentrañado la visión iusinformática del derecho a la intimidad en sus decisiones de protección del derecho de la intimidad, información y habeas data (C.C. Sents.T-414/ 1992, Ago.T-444/92 de 7Jul. T-127/1994, de 15 de Mar.), derecho de ha- beas data (CC. T-022/1993, de 29 Ene.), el derecho al buen nombre (C.C. Sent. T-413/ 1993, de 29 de Sep.), derecho a la información, la intimidad y el habeas data (CC.Sent. T-097/1995, de 3 de Mar. Sent SU-082 y 089/1995, de 1 de Marz.), el derecho de "autodeterminación informática" (C.C. Sent.T-552/1997, de 30 de Oct), etc.

Veamos ahora, las normas prototipo de cada generación.

4.2. ALEMANIA: LA LEY FEDERAL DE PROTECCION DE DATOS DE 27 DE ENERO DE 1977 [136].

---

(135) Véase, parte III, punto 5 y ss.
(136) Texto completo en AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla. núm.2.

Esta Ley Federal es el resultado de la estructuración y promulgación de la Ley perteneciente al *Land de Hesse* de 7 de Octubre de 1970, primera en regular todo lo atinente al tratamiento informatizado de datos que "utilizaban los servicios administrativos del Land" y de la ley de la Renania-Palatinado [137]

La Ley Federal de protección de datos, no sólo fue la pionera a nivel internacional en regular legislativamente el tratamiento informatizado de los datos personales, sino que es la primera y la única, incluso hasta épocas actuales, en tratar integralmente todo lo atinente al tratamiento informatizado los datos personales, tanto en el ámbito público como privado; así como también en regular los aspectos civiles, penales y derecho público derivados del ejercicio, protección y transgresión de los derechos que ostentan los titulares de los datos, ante las autoridades civiles, administrativas y punitivas.

La Ley Federal Alemana de protección de los titulares de los datos, el 20 de diciembre de 1990, recibió una nueva redacción en su texto y que en esencia su contenido y su "concepción sigue siendo igual a la de 1997" [138] . Por ello, estudiaremos brevemente el texto de 1977. Esta ley (en adelante LFAPD), tiene cinco secciones de las que destacaremos los aspectos que tienen que ver con el objeto de nuestro trabajo. Son:

SECCION PRIMERA: Disposiciones generales: En las que se refiere a los cometidos y objeto de la ley, definiciones, admisibilidad del "proceso de datos", derechos del "afectado"; y, "secreto de los datos, medidas técnicas y de organización".

SECCION SEGUNDA: Proceso de datos de autoridades y otros servicios públicos: ámbito de aplicación; elaboración de datos personales por cuenta ajena; almacenamiento y modificación de datos; comunicación de datos dentro del sector

público; comunicación de datos a “entes” ajenos a un sector público; Publicidad de los datos almacenados; Facilitación de información “al afectado”; Rectificación, bloqueo y cancelación de datos; Ejecución de la protección de datos en la Administración Federal; Disposiciones administrativos de carácter general; nombramiento de un

---

(137) ORTI VALLEJO, A. Ob. cit. pág. 12
(138) Según Heredero Higueras, citado por ORTI VALLEJO, Ob. ut supra cit., pág. 12-13.

Comisario Federal de Protección de datos; situación jurídica del Comisario Federal de Protección de Datos; Funciones del Comisario Federal de Protección de Datos; Reclamaciones del Comisario Federal de Protección de Datos; y , Recurso ante el Comisario Federal de Protección de Datos.

SECCION TERCERA: Proceso de datos de entes no público para uso interno: Ambito de aplicación; modificación de datos; facilitación de información al afectado; Rectificación, bloqueo y cancelación de datos; Designación de un Comisario de Protección de Datos; Funciones del Comisario de Protección de Datos; y, Autoridad de tutela.

SECCION CUARTA: Proceso de datos realizado con finalidad mercantil para entes no públicos: Ambito de aplicación; Almacenamiento y comunicación de datos; modificación de datos; facilitación de información al “afectado”; Rectificación, bloqueo y cancelación de datos; elaboración de datos personales para su difusión en forma “anonimizada” (o simplemente anónima); elaboración de datos personales por cuenta ajena; Comisario de Protección de Datos; Deber de denuncia; y, Autoridad de tutela.

SECCION QUINTA: Normas punitivas y sancionadoras: Acciones punibles, y, Infracciones de Policía.

SECCION SEXTA: Disposiciones transitorias y finales: Disposiciones finales; Aplicación de la Ley de Procedimiento Administrativo; Disposiciones subsistentes; “Cláusula Berlinesa”; y , entrada en vigor.

Son muchos y variados los temas los que aborda la Ley alemana, sin embargo, destacaremos a nuestros efectos investigativos los siguientes, los cuales los dividiremos así: a) Las definiciones técnico-jurídicas iusinformáticas; b) El Comisario de Protección de los Datos; y c) El Sistema Punitivo y Sancionador en materia de datos.

4.2.1. DEFINICIONES TECNICO-JURIDICAS IUSINFORMATICAS.

La Ley Federal Alemana del tratamiento de datos personales, inaugura en su condición de pionera, la técnica legislativa que posteriormente se extendiera en toda norma jurídica estatal y comunitaria de iniciar el texto legislativo con un glosario de términos técnico-jurídicos cerrados, cuyas definiciones son de aplicación necesaria para todo operador jurídico de la ley. Las definiciones contenidas en la Ley de 27 de Enero de 1977, son *iusinformáticas*, por referirse a la órbita jurídica tanto al derecho público como al derecho privado y en particular, al tratamiento informatizado de datos dominado por la informática.

Las diversas definiciones las podemos agrupar por su contenido y afinidad con el fenómeno tecnológico de la informática (entendida como la ciencia del tratamiento lógico, sistematizado e informatizado de cualquier unidad de información o datos) y el derecho, en los siguientes: a) Definiciones sobre los sujetos del tratamiento de datos; b) Definiciones aplicables al "*Habeas Data*" y al proceso de datos personales; y, c) Definiciones aplicables al procedimiento informatizado de datos.

4.2.1.1. DEFINICIONES SOBRE LOS SUJETOS DEL TRATAMIENTO DE DATOS.

Pertenecen a este grupo las definiciones de "Datos personales", "tercero"y "ente almacenante". *Datos personales* se consideran las indicaciones concretas acerca de condiciones personales o materiales de una persona natural determinable (o "afectado", aunque en puridad sería el interesado o titular de los datos). Estos datos personales como información perteneciente a cualquier persona física, incluye tanto la contenida en método no informáticos, como en aquellos a los que se les ha aplicado la técnica, tratamiento o procedimientos informatizados o "*procedimientos*

automáticos", como lo denomina la Ley Federal Alemana de Protección de Datos. Se excluyen no del concepto de datos personales sino del ámbito de aplicación de la LFAPD, los datos personales elaborados por empresas auxiliares de la prensa, radio o cinematografía, exclusivamente para uso interno en relación con la difusión (Art. 1 *in fine* LFAPD), salvo en lo atinente a las "medidas técnicas y de organización" que éstas deben implementar para garantizar los derechos e intereses legítimos de los titulares de los datos de conformidad con LFAPD **[139]**.

---

(139) "Si se elaboraren automáticamente datos personales, deberá adoptarse para la aplicación de los preceptos de la presente ley medidas que en función de la índole de los datos personales que hubieren de ser protegidos fueren idóneas para: l. impedir a personas no autorizadas el acceso a los equipos de proceso de datos con los cuales fueren elaborados los datos personales (control de acceso a los equipos); 2. impedir que las personas ocupadas en la elaboración de datos personales retiren sin autorización soportes de información (control de salidas); 3. impedir la introducción no autorizada en memoria de datos personales, así como la toma de conocimiento, modificación o cancelación no autorizadas de datos personales ya almacenados (control de memorias); 4. impedir que personas no autorizadas utilicen sistemas de proceso de datos a partir de los cuales se comunicaren datos personales valiendose de (…)

Tercero, es toda aquella persona o entidad ("ente") ajena a la entidad almacenante, a excepción de los interesados o de aquellas personas y entidades (Autoridades públicas, personas jurídicas, sociedades u otras agrupaciones, etc) que obraren por "encargo" dentro del ámbito de vigencia de la LFAPD.

Y, finalmente, *Entidad Almacenante*, se consideran como tales cualquiera de las personas naturales o jurídicas o entidades que almacenaren datos por sí mismo o enco-comendare a otro su almacenamiento. Estas son: a) Las diversas Autoridades o entidades públicas (pertenecientes al Estado, a los Municipios, mancomunidades de municipios y cualquier otras personas jurídicas de derecho público sujetas a tutela estatal. Art. 7 LFAPD); y, b) Personas naturales o jurídicas, sociedades u otras agrupaciones de personas de derecho privado, para uso interno (se exceptúan de ésta aparte las personas de derecho privado que desempeñan "funciones propias de la Administración Pública". Art.22 LFAD), o las que realicen "con carácter regular y por cuenta ajena" actividades con "finalidad mercantil" (en esta se incluyen las empresas de derecho público, con idéntica finalidad. Art. 31 LFAPD).

4.2.1.2. DEFINICIONES APLICABLES AL "HABEAS DATA" Y AL PROCESO DE DATOS PERSONALES.

Si bien como recuerda el profesor *González Navarro*, citando a *Heredero Higueras* [**140**], el derecho de acceso, aún antes de la promulgación de las leyes de protección de datos, fue bautizado como *habeas data*, por considerarlo como una

---

Continuación cita No. **139**

dispositivos automáticos o en los cuales se introdujeren datos personales valiendose tales dispositivos (control de usuarios); 5. garantizar que las personas con derecho a usar un sistema de proceso de datos puedan acceder mediante dispositivos automáticos exclusivamente a los datos personales que estuvieren comprendidos dentro del ámbito de su facultad de acceso (control de acceso a los datos) ; 6. garantizar que se pueda comprobar y determinar en que puntos es posible comunicar datos personales valiendose de dispositivos automáticos (control de la comunicación); 7. garantizar que se pueda comprobar y determinar a posteriori que datos personales, en que momento y por quien fueron introducidos en sistemas de proceso de datos (control de la introducción en memoria); 8. garantizar que en los datos personales que fueren elaborados por cuenta ajena sólo puedan serlo de conformidad con las instrucciones del comitente (control de encargos); 9. garantizar que en los supuestos de comunicación de datos personales, así como en los casos de transporte de los correspondientes soportes de información, estos no puedan ser leídos, modificados o cancelados sin autorización (control del transporte de datos); 10. configurar la organización interna de las autoridades o empresas de tal manera que la misma responda a las exigencias de la protección de datos (control de la organización)". ANEXO AL ARTICULO 6, PRIMER PARRAFO, PROPOSICION PRIMERA.

(140) GONZALEZ NAVARRO, Francisco. *DERECHO ADMINISTRATIVO ESPAÑOL*. Ed. Eunsa, 1a., ed., 1987 y 2a., ed., 1994, Pamplona, pág. 179

modalidad de acción exhibitoria análoga a la del *habeas corpus* del derecho anglosajón, no debemos olvidar que el derecho de acceso a los datos, sobre todo los informatizados o sometidos en parte o en todo a tratamiento o procedimientos "automatizados", conlleva un grupo de derechos concomitantes y subsiguientes al ejercicio del derecho de acceso, tales como: el derecho a conocer la existencia de datos que le conciernan a la persona y que se hallen almacenados ("storage") y contenidos en un fichero, banco de datos o simplemente en un "archivo" o registro informatizado (o simplemente "*file*" anglosajón), bien sean procesados con o sin su consentimiento; así como también el derecho a consultarlos, si fuere del caso, por cualquier método, técnica o medio informático, electrónico o telemático [**141**] , dentro de conformidad con el ordenamiento jurídico vigente sobre la materia. Como consecuencia, de ello podrá, independientemente de los recursos (básicamente jurisdiccionales), solicitar la revisión, rectificación, actualización, modificación y, llegado el caso, la cancelación, borrado y bloqueo de los datos persona nales que le conciernan.

En consecuencia, pertenecen a este segundo grupo de definiciones, las siguientes: almacenar, comunicar, modificar y cancelar datos personales.

Almacenar datos personales, en términos iusinformáticos, consiste en recoger, registrar o conservar en un soporte de información con miras a su ulterior utilización. El "almacenamiento" de datos, según la LFAPD constituye una fase del procedimiento informatizado de datos que abarca una etapa previa, como es la recolección; una etapa concomitante, como es la del registro; y una etapa posterior, como es la conservación de datos. Todas ellas interdependientes, pues faltando una de éstas no se puede completar el fenómeno o actividad de almacenamiento.

La LFAPD, establece la subsidiariedad de ésta, cuando existan leyes especiales federales sobre los datos personales almacenados en registros informatizados (art.45), destacando con ello la etapa de almacenamiento y tratamiento informatizado de los datos. Así a título de ejemplo, se aplicará la ley especial sobre la general en la guarda de secreto sobre noticias obtenidas oficialmente o en el ejercicio profesional; p. e., el art. 12 de la Ley de Estadísticas para fines Federales, de 3 de Sep

---

(141) Véase, parte III y IV de esta investigación al respecto.

tiembre de 1953 **[142]**.

La LFAPD, al hacer mención a los derechos que tiene el "afectado" (por titular de los datos, en términos positivos y no en términos negativos, tal y como lo prevé la ley) dentro del llamado "proceso de datos", se hace expresa referencia a los derechos derivados del acceso y consulta de la información y subsecuente, todos ellos componentes del derecho fundamental del *habeas data*. Los derechos subsecuentes son: a) La información acerca de los datos almacenados en relación con la persona; b) La Rectificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; c) El bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y d) La cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien --a elección, ademas del derecho de cancelación-- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

Comunicar, en términos de la LFAPD, es una especie cualificada (dirigida a "terceros") del género *informar* (que la ley denomina derecho de "facilitación de información al afectado", considerado como un derecho fundamental, no absoluto que tiene el titular de los datos personales, tanto en el proceso de datos público [14 3], como

---

(142) Otros ejemplos son: a) Sobre limitación del examen de documentos por terceros; p. e., el articulo 61, párrafo segundo y tercero de la ley de estado civil de las personas; b) Sobre examen del expediente personal por los funcionarios o empleados; p e., el articulo 90 de la ley federal de funcionarios; el articulo 83 de la ley de Organización de Empresas; c) Sobre el deber de las autoridades de informar a los ciudadanos de los datos almacenados acerca de los mismos; p. e., el articulo 1.325 de la Ordenanza Imperial del Seguro; g) Sobre difusión, rectificación y cancelación de los datos referidos a personas incluidos en Registros públicos; p. e., los artículos 19, 23, 27, segundo párrafo; y d) Sobre la obligación de elaborar datos referidos a personas en la rendición de cuentas, comprendidas la contabilidad y otras anotaciones; p.e., los artículos 38 a 40, 42 a 47 del Código de Comercio. Texto completo de la LFAPD., en AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla. Tratados Internacionales núm. 2

(143) Se facilitará al afectado, si así lo solicitare, información acerca de los datos almacenados con relación a su persona. En la solicitud deberá detallarse la índole de los datos personales sobre los cuales deba facilitarse la información. El servicio o ente almacenante determinará el procedimiento, en especial la forma de facilitar información según las conveniencias del servicio... No precederá la facilitación de la información en los siguientes supuestos: 1. si la información perjudicare el legítimo cumplimiento de las tareas comprendidas en la competencia del servicio almacenante; 2. si la información perjudicare a la seguridad o al orden públicos o causare detrimento a la Federación o a un Estado; 3. si los datos personales o el hecho de su almacenamiento hubieren de ser mantenidos en secreto en virtud de norma jurídica o por razón de su esencia, en especial en razón del interés legítimo preponderante de un tercero ; 4. si la información hiciere referencia a la comunicación de datos personales a las autoridades mencionadas en el articulo 12, segundo párrafo, apartado 1. La facilitación de la información estará sujeta al devengo de una tasa... (art. 13 LFAPD).

en el privado [144], puesto que se prevé expresas excepciones al ejercicio del mismo), puesto que comunicar se entiende la acción de dar a conocer a terceros datos almacenados u obtenidos directamente mediante un proceso de datos, tanto si fueren datos difundidos por el ente almacenante, como si son datos conservados por la entidad para su examen, en especial para su búsqueda automática (art. 4-2). En este sentido, la *comunicación* de datos personales, con el lleno de los requisitos previstos en la ley, bien puede hacerse a personas como entidades públicas tanto en los procesos de datos de carácter público (art. 11), como en los procesos de índole privada (art. 32).

Cancelar es la acción de hacer irreconocibles datos ya almacenados: cualquiera que fuere el procedimiento empleado a tal efecto. En tanto *modificar*, se considera la acción de transformación del contenido de datos ya almacenados (art. 4-3 y 4-4). En el caso de los datos de carácter privado, la *modificación de los datos* personales será admisible dentro del marco de los fines de una relación contractual o de una relación de confianza análoga a la relación contractual creada,

respectivamente con el titular de los datos, o en la medida en que fuere necesaria para salvaguardar intereses legítimos de la entidad almacenante, y no existiere motivo fundado para creer que de ello pudieren resultar perjuicios para los intereses dignos de protección del interesado (art. 25).

La *Rectificación, bloqueo y cancelación de datos*, son tres acciones íntimamente ligadas y subsecuentes por la consideración de sí los datos almacenados,

---

(144) Si se almacenaren por primera vez datos referentes a la persona del afectado, deberá este ser informado de ello, a menos que hubiera tenido conocimiento del almacenamiento por otros medios. El afectado podrá e- xigir información acerca de los datos almacenados con relación a su persona. Si los datos fueren objeto de tratamiento automático, el afectado podrá exigir asimismo información acerca de las personas y servicios a los cuales fueren transmitidos regularmente sus datos. Deberá señalar la clase de los datos personales sobre los cuales debiere ser facilitada la información. La información se facilitara por escrito, siempre que no procediere otra forma de facilitación de información en razón de especiales circunstancias. Podrá exigirse por la información una retribución, la cual no Podrá exceder de los gastos directamente imputables a la facilitación de la información. No Podrá exigirse retribución en los casos en que por circunstancias especiales existiere motivo fundado para creer que se ha llevado a cabo un almacenamiento inexacto o ilícito de datos personales, o en los casos en que la información facilitada hubiera revelado que los datos personales debieren ser rectificados o, en virtud de lo dispuesto en el articulo 27, tercer párrafo, proposición segunda, semiproposición primera, hubieren de ser cancelados. Los párrafos primero y segundo no regirán en la medida en que: 1. el dar a conocer datos referidos a personas pudiera crear un peligro considerable para el objeto social o los fines del ente almacenante, y no obstaren a ello intereses legítimos del afectado, 2. el servicio publico competente con relación al ente almacenante hubiere observado que el dar a conocer datos referidos a personas podría poner en peligro la seguridad o el orden públicos o causar otros perjuicios para el bien de la Federación o de un Estado, 3. los datos personales hubieren de ser mantenidos en secreto en virtud de una norma jurídica o por razón de su esencia, en especial a causa de intereses legítimos preponderantes de una tercera persona, 4. los datos personales hubieren sido tomados de fuentes de acceso general, 5. los datos personales que, en virtud de lo dispuesto en el articulo 27, segundo párrafo, proposición segunda, estuvieren bloqueados porque sobre la base de disposiciones legales, estatutarias o contractuales, no pudieren ser cancelados a tenor de lo dispuesto en el articulo 27, tercer párrafo, proposición primera (art. 26 LFAPD).

son : a) inexactos o se duda sobre su exactitud. El *in dubio pro date*, como podríamos llamarlo siempre favorece al titular de los datos. b) Si han sido almacenados de forma ilícita, c) Si los datos dejado de ser necesarios para los fines para los cuales fueron almacenados; y, d) porque así “lo exige” el titular de los datos (“afectado”).

Sin embargo, la rectificación de los datos sólo es procedente en el caso de no ser exactos los datos personales (art. 14 y 27 *ab initio*).

Se procederá al bloqueo de datos, cuando su exactitud fuere discutida por el titular de los mismos y no fuere posible determinar su exactitud ni su inexactitud. Igualmente serán bloqueados los datos cuando su conocimiento hubiere dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas

a éste encomendadas, a menos que fueren imprescindibles para fines científicos, para fines probatorios, “intereses preponderantes del servicio almacenante o de un tercero”, o por consentimiento del titular de los datos. Esto rige para los datos con carácter público como los de carácter privado.

La cancelación de datos, en los datos de carácter público, procederá cuando su conocimiento hubiere dejado de ser necesario para que el servicio almacenante pueda cumplir debidamente las tareas comprendidas dentro de su competencia y no existieren motivos fundados para creer que la cancelación pudiera causar perjuicio a intereses dignos de protección del titular. Igualmente serán cancelados los datos si su almacenamiento hubiere sido ilícito o cuando así lo exigiere el interesado. En los datos de carácter privado, además de los anteriores casos, procederá la cancelación cuando así lo exigiere el interesado, en los datos referentes a condiciones de salud, acciones punibles, infracciones de policía, así como a concepciones religiosas o políticas, si su exactitud no pudiere ser probada por la entidad almacenante (art.14 y 27 *in fine*).

El *habeas data* y el grupo de derechos subsecuentes rigen para los titulares de datos cuando sean almacenados tanto en un “proceso de datos de autoridades y otros servicios públicos” (art.7 y ss LFAPD), o procesos informatizados de carácter público, como en los “ procesos de datos de entes no públicos para uso interno “ (art. 22) y los “procesos de datos realizados con finalidad mercantil para entes no públicos”, vale decir de carácter privado o que se reputan privados a los efectos de la LFAPD, respectivamente (v.gr. el caso de las “empresas públicas de derecho público”, art.31).

4.2.1.3. DEFINICIONES APLICABLES AL PROCESO INFORMATIZADO DE DATOS.

La LFAPD, estructura tres procesos de datos, a saber: a) El Proceso de datos de autoridades y servicios públicos (arts. 7 a 21); b) El proceso de datos de “entes” no públicos para uso interno (arts. 22 a 30); y c) El proceso de datos realizado con finalidad mercantil para entes no públicos (arts. 31 a 40). En estos procesos de datos de naturaleza jurídica de derecho público y de derecho privado, respectivamente, rige por igual etapas o fases, principios, derechos y deberes de los titulares de los datos, a pesar de estar regulados por separado, pues la misma norma reiterada como

innecesariamente los reglamenta para cada uno, con específicas diferencias v.gr. sobre el derecho de "facilitación de información al afectado" (arts. 14, 27 y 34), con cuasi similar contenido para cada uno de los procesos.

Interesa a los propósitos de la investigación, desentrañar las etapas ínsitas en dichos procesos, cara a la estructuración del procedimiento informatizado de datos informáticos, el cual abordaremos en la Parte III, *in fine.*

En efecto, las etapas o fases inmersas en el *proceso alemán de datos* inmersa en las tres clases de procesos de datos son: a) La etapa de recolección o de "elaboración" de datos; b) La etapa de almacenamiento; c) La etapa de conservación e inscripción en un registro (público, privado o mixto, según fuere el caso); y d) La transmisión o comunicación de datos; y e) Rectificación, bloqueo y cancelación de datos [**145**].

La LFAPD, al hablar del proceso de datos, en general, estipula que a éste debe someterse los titulares de los datos o interesados, si así esta previsto en una ley o norma jurídica en forma expresa o si el interesado así lo consiente en forma escrita, "siempre que no procediere otra forma en razón de especiales circunstancias" (art. 3 LFAPD).

Igualmente, interesa aquí destacar los conceptos estructurales del derecho de habeas data y el de "archivo informatizado" que están íntimamente ligados con el concepto de proceso de datos. En efeto, se considera *archivo informatizado*, una colección de datos estructurados de manera homogénea, susceptibles de ser obtenidos y ordenados de conformidad con determinadas características y, en su caso,

---

(145) En la parte III, *in fine* de esta investigación proponemos una estructura de procedimiento informatizado de datos personales, basado en estas concepciones de la LFAPD y las emitidas por los doctrinantes Fermín Morales Prats y Vittorio Frosini.

reordenados y explotados de conformidad con otras características determinadas, cualquiera que fuere el procedimiento empleado a tal efecto, sin se consideren comprendidos los expedientes y las colecciones de expedientes, a menos que los mismos pudieren ser reordenados y explotados por procedimientos automáticos (art. 1-3).

Ahora, pasemos a ver otros aspectos capitales del procedimiento informatizado de datos alemán que aún hoy, tienen relevancia y discusión doctrinal no pacífica.

4.2.2. EL COMISARIO DE PROTECCIÓN DE LOS DATOS: UN OMBUSDMAN [146] EN EL SECTOR PUBLICO Y UN VEEDOR CIUDADANO EN EL SECTOR PRIVADO.

La figura del Comisario de datos personales en el proceso de datos alemán se estructura, cualifica y funciona, según la clase de proceso (público o privado) ante el cual se nombra o se designa por parte de las autoridades públicas federales o las personas privadas competentes, según fuere el caso y ámbito competencial.

4.2.2.1. EL COMISARIO FEDERAL DE PROTECCION DE DATOS EN EL SECTOR PUBLICO.

El nombramiento del Comisario Federal de protección de datos en "los procesos de datos de autoridades y otros servicios públicos", se realiza por el Presidente Federal a propuesta del Gobierno Federal. El nombramiento se extingue por expiración del plazo de mandato y por destitución, previo trámite legal y la entrega de un "instrumento fehaciente" extendido por el Presidente Federal.

El designado como Comisario prestará su juramento y cumplirá un plazo de cinco (5) años y su régimen jurídico será el de derecho público. Jerárquicamente depende el Ministerio Federal del Interior, quien podrá entre otras atribuciones, encomendar a un sustituto del Comisario, cuando el titular se viere impedido para ejercer el cargo.

El Comisario Federal de Protección de Datos, tiene las siguientes funciones:

---

(146) ORTI VALLEJO, A. Ob. ut supra cit., pág. 13

a) *De cumplida ejecución y de asesoramiento sobre leyes de protección de datos*. En consecuencia, velará por la observancia y cumplimiento de la LFAPD; así como de otros preceptos sobre protección de datos a los cuales están obligados las autoridades públicas y otros servicios públicos de la Federación, para

corporaciones, instituciones y fundaciones de derecho público, etc. Se exceptúa de esta previsión los Tribunales, en la medida en que estos no conocieren de negocios contencioso-administrativos. A este efecto podrá formular recomendaciones en orden al mejoramiento de la protección de datos, pudiendo en especial asesorar al Gobierno Federal y a los distintos Ministros, así como a las restantes autoridades públicas en todo lo tocante a la protección de datos.

b) *De Emisión de dictámenes e informes*. Si fuere requerido a ello por "la Dieta Federal Alemana "o por el Gobierno Federal, el Comisario Federal deberá emitir dictámenes e informes. Asimismo elevara anualmente a la Dieta Federal Alemana una memoria de su actividades.

c) *De solicitud de auxilio a autoridades y servicios públicos*. El Comisario podrá solicitar a las autoridades y servicios públicos le faciliten información en relación con las preguntas que éste formulare, así como facilitarán el examen de toda clase de documentos y expedientes que guardaren relación con la elaboración de datos referidos a personas, especialmente los datos almacenados y los programas de ordenador. Y, como consecuencia, permitirán en todo momento el acceso a todos los locales oficiales.

d) *De Registro*. EI Comisario Federal llevará un registro de los archivos explotados automáticamente, en los cuales se almacenaren datos referidos a personas. Dicho registro se limitará a contener un cuadro general de la naturaleza de los archivos y de los fines para los cuales fueren empleados. El registro podrá ser examinado por toda persona. Las autoridades, servicios y entidades públicas, estarán obligadas a denunciar al Comisario Federal los archivos explotados automáticamente por las mismas. Quedan exentos de esta obligación : La Oficina Federal de Defensa Constitucional, el Servicio Federal de Investigación y el Servicio de Contraespionaje Militar (art. 19).

e) *De reclamaciones*. Si el Comisario Federal de Protección de Datos observare que con ocasión del proceso de datos personales se atenta contra LFAPD, o contra las normas jurídicas de protección de datos, formulará una reclamación ante la autoridad suprema federal competente, si se tratare de la Administración Federal; ante la Dirección del Ferrocarril Federal, si se tratare de este; ante la Dirección o, en

su caso, ante el órgano que tuviere atribuida la representación, si se tratare de corporaciones, instituciones o fundaciones de Derecho publico directamente dependientes de la Federación, así como si se tratare de agrupaciones de tales corporaciones, instituciones y fundaciones; y la intimara a que se pronuncie dentro de un plazo que el mismo fijara (art. 20).

f) *De protección de los derechos de los titulares de datos personales*. Toda persona podrá acudir al Comisario Federal de Protección de Datos si fuere de la opinión de que en el curso del tratamiento de sus datos personales realizado por las autoridades, servicios y entidades públicas, a excepción de los Tribunales, siempre que estos no conocieren de negocios contencioso-administrativos, han lesionada los derechos de aquéllas (art. 21).

4.2.2.2. EL COMISARIO DE PROTECCIÓN DE DATOS EN EL SECTOR PRIVADO.

La LFAPD, si bien distingue los "procesos de datos de entes no públicas para uso interno" y los "procesos de datos realizados con finalidad mercantil para entes no públicos", no procede de idéntica manera, cuando menos, respecto de las funciones generales y especiales que el Comisario de Protección de los datos en el sector privado debe cumplir en uno y otro procesos.

En efecto, cuando se trata de procesos de datos de entes no públicos para uso interno, la designación del Comisario de Protección de datos se realizará, según el art. 28 de la LFAPD, por las personas, sociedades y otras agrupaciones de personas de derecho privado que sometan a tratamiento (o elaboraren) automáticamente datos personales y a tal efecto ocuparen con carácter permanente, por regla general, a cinco trabajadores por lo menos, deberán nombrar por escrito, lo mas tarde dentro de un mes después de iniciar su actividad, a un Comisario de Protección de Datos. Igual se procederá si se ocupare con carácter permanente a veinte trabajadores.

El Comisario de Protección de Datos dependerá directamente del propietario, de la Dirección, del gerente o de otra persona a quien correspondiere la dirección en virtud de disposición legal o estatutaria. En la aplicación de su pericia profesional en

materia de protección de datos no estar sujeto a instrucciones superiores. No podrá ser objeto de perjuicios por razón del cumplimiento de sus funciones.

El Comisario de Protección de Datos, cuando se trata de "procesos de datos realizados con finalidad mercantil para entes no públicos", se designará por las personas, sociedades y otras agrupaciones de personas de derecho privado, o en su caso, por las empresas de derecho público que concurrieren en el mercado, según el art. 38 de la LFAPD. En cuanto a las funciones generales y especiales, éste Comisario cumplirá, en cuanto fuere procedente, las que se atribuyen al Comisario en el proceso de datos de entes no públicos para usos internos.

En tal virtud, El comisario de Protección de Datos, para uno y otro proceso de datos, cumple en su ámbito competencial idénticas funciones generales a las atribuida al Comisario Federal de Protección de Datos; vale decir, que velará por la observancia, cumplimiento y conocimiento de la LFAPD; así como de otras disposiciones relativas a la protección de datos. A tal efecto podrá acudir en casos de duda a la Autoridad de tutela (autoridades administrativas o jurisdiccionales, según el caso).

Como funciones especiales tendrá: a) *De veeduría y vigilancia de datos, fines, destinatarios y equipos.* En tal virtud, llevará un estado de la clase de los datos personales almacenados, así como del objeto social y los fines para cuya realización o cumplimiento fuere necesario conocer tales datos, de sus destinatarios regulares y la clase de los equipos de tratamiento automatizado de datos que estuvieren instalados;

b) *De veeduría de medios informáticos.* Velará por la regularidad de la aplicación de los programas de ordenador con cuya ayuda debieren ser tratados los datos personales; y,

c) *De veeduría profesional.* Prestan asesoramiento en la selección de las personas que se hubieren de ocupar en el tratamiento de datos los personales.

4.2.3. SISTEMA PUNITIVO Y SANCIONADOR EN MATERIA DE DATOS PREVISTO EN LA LFAPD.

Siendo la LFAPD, una ley de ámbito federal, su carácter es de ley general, por tanto, se aplicará subsidiariamente en caso de ausencia de ley especial o para llenar vacíos o lagunas legislativas si existieren otras leyes de protección de datos de ámbito federal (art. 45). En materia punitiva se aplicarán preferentemente a la LFAPD, a título de ejemplo las siguientes disposiciones: a) Sobre el derecho a negarse a extender certificaciones o a facilitar información por razones personales o profesionales en procedimientos judiciales (arts. 52 a 55 de la Ordenanza Procesal Penal); b) Sobre la obligación, limitación o prohibición del almacenamiento, difusión o publicación de indicaciones pormenorizadas sobre personas (art. 161 de la Ordenanza Procesal Penal); y, c) Secreto profesional (v.gr. secreto médico. Art. 203 Código Penal) [147].

Sin embargo, la LFAPD, se aplicará con carácter general en los casos expresamente previstos como hechos punibles (delitos y contravenciones) contra el tratamiento (informatizado o no) de datos personales.

1. Delitos (art. 41 LFAPD):

a) *Atentados contra los datos personales que no son de dominio público.*

Se considera como hecho punible, perseguible a instancia de parte el que sin la debida autorización: 1. comunicare o modificare, o 2. recuperare o se procurare a partir de archivos encerrados en depósitos adecuados, datos referidos a personas y protegidos por la LFAPD, que no fueren de dominio público, será castigado con pena de privación de libertad de un año como máximo o con pena de multa.

b) *Tipo Agravado por el lucro o por perjuicio a otro.*

Si el autor, realizare una cualesquiera de la anteriores conductas y además obrare por precio o con el propósito de procurarse a si mismo o a otro un lucro o de causar perjuicio a otro, la pena será privativa de libertad de dos años como máximo o de multa.

2. Contravenciones o “Infracciones” de policía (art. 42 Ibídem). Obra con dolo o culpa quien: a) *Por falta de información al interesado de almacenamiento de datos que le conciernen*. No informar al interesado (“afectado”), sobre el almacenamiento de datos personales que le conciernen por primera vez , a menos

que hubiere tenido conocimiento del almacenamiento por otros medios. Igual incumplimiento se dará, si

---

(147) Véase otros ejemplos en el apartado 4.2.1

por primera vez fueren comunicados datos acerca de la persona interesada, siendo que debía ser informada de su almacenamiento, a menos que hubiere tenido noticia de éste por otros medios.

b) *Por falta de designación, teniendo la obligación de hacerlo, de un Comisario de Protección de datos.* Por incumplimiento de designar un Comisario de Protección de datos, por parte de las personas, sociedades y agrupaciones de derecho privado que sometan a tratamiento informatizado datos personales y que ocuparen permanentemente trabajadores (cinco o veinte). Igual, sucederá cuando se incumple la obligación de designar Comisario de Protección de datos por parte de las personas, sociedades y agrupaciones de derecho privado dentro de los procesos de datos realizado con finalidad mercantil para entes no públicos.

c) *Por falta de adjunción de motivos que justifiquen un interés legítimo para la comunicación de datos*. Si el destinatario no justificare los motivos y la existencia de un interés legítimo y los medios que lo acreditaren en forma fidedigna y detallada para que sea admisible la comunicación de datos personales.

d) *Por falta de cumplimiento del "deber de denuncia"*. Cuando las personas, sociedades y otras agrupaciones de personas de derecho privado, así como sus filiales y sucursales, teniendo la obligación de formular en tiempo oportuno (un mes) denuncia, no lo hacen. Igual incumplimiento se verificará, si estas personas no facilitaren al formular tal declaración los datos necesarios o no los facilitaren correctamente o de manera incompleta. Estos datos se refieren a la determinación del propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y sobre personas encargadas de la dirección del tratamiento de datos y sus direcciones (art.39-2 y 3 LFAPD) **[148]**

---

(148) *LFAPD. ART. 39. Deber de denuncia*. Las personas, sociedades y otras agrupaciones de personas que se mencionan en el articulo 31, así como sus filiales y sucursales, deberán dar cuenta de la iniciación de su actividad ante la autoridad de tutela competente dentro del plazo de un mes. Al Llevar a cabo la denuncia, deberán comunicarse al Registro llevado por la Autoridad de tutela los siguientes datos: 1. nombre o

denominación del ente; 2. propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y personas encargadas de la dirección del tratamiento de datos; 3. dirección; 4. objeto social o fines del ente y del tratamiento de datos; 5. naturaleza de los equipos utilizados para el tratamiento automatizado de datos; 6. nombre del Comisario de Protección de Datos; 7. naturaleza de los datos personales almacenados por el ente o por encargo suyo; 8. en caso de comunicación regular de datos personales, destinatarios y naturaleza de los datos comunicados. El primer párrafo regirá en cuanto fuere procedente para la terminación de la actividad, así como para la modificación de los datos facilitados en virtud de lo dispuesto en el segundo párrafo.

e) *Por incumplimiento en la facilitación de información pertinente o no tolerase el acceso a terrenos y locales para ante la Autoridad de Tutela.* Las personas, sociedades y otras agrupaciones de derecho privado, que teniendo la obligación de facilitar sin demora, si fueren requeridas para ello, las informaciones necesarias para el complimiento de las funciones de la Autoridad de Tutela, no facilitare una información o no la facilitare correcta o completamente, o no la facilitare en tiempo oportuno, o, incumpliendo las funciones de vigilancia encomendadas por la Autoridad de Tutela para penetrar en los inmuebles y locales de negocio del ente, y llevar a cabo en ellos inspecciones y comprobaciones y para examinar documentos de la explotación, en especial el estado que debiere ser llevado por el Comisario de Protección de Datos, y examinar los datos almacenados y los programas de tratamiento

La conducta antirreglamentaria podrá ser sancionada con pena de multa de cincuenta mil marcos alemanes como máximo.

4.3. LA EUROPA DE 1980: EL COMIENZO DE UNA DÉCADA CLAVE EN LA NORMATIZACIÓN Y NORMALIZACIÓN DEL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES.

Si bien es cierto Alemania, Suecia, Francia; entre otros Estados europeos, habían afrontado no solo teórica sino prácticamente el complejo mundo del tratamiento informatizado de datos de carácter personal, como el movimiento, flujo o circulación de datos entre países, expidiendo leyes sobre la materia; no es menos cierto también, que éstos esfuerzos legislativos resultaban aislados e incomprensibles incluso en el contexto de una Europa unida, pregonada y defendida desde hacía tres décadas antes con la suscripción de Francia y Alemania con la

llamada “declaración o Plan Shuman” de 1950, y subsiguientemente la suscripción del “Tratado del Carbón y el Acero” de 1951--CECA--, por los países bajos, Italia, Bélgica, Luxemburgo y la entonces República Federal Alemana (RFA). Mucho más, resultaba incomprensible cuando dichos Estados habían apostado por una Comunidad de Estados europeos, de origen económico sí, pero luego su radio ampliado a los aspectos sociales, laborales, culturales, políticos, legislativos; y en fin, en un futuro no muy lejano, alcanzar lo siempre buscado: un gran Estado Europeo unido con una sola Constitución, como lo teoriza el profesor alemán de la Universidad de Münster, *Martín Seidel* **[149]**

Pese a ello, el profesor *Davara* **[150]**, sostiene que desde 1967 en Europa existía “conciencia europea sobre protección de la privacidad” (por la traducción literal de la “privacy” anglosajona) y para ello relaciona varias recomendaciones surgidas en el seno del Consejo de Europa, el cual constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona, entre los que estaba la Intimidad. Entre las más destacadas están: a) La Resolución 509 de 1958, de la Asamblea del Consejo de Europa, sobre “Derechos Humanos y los nuevos logros científicos y técnicos”, b) Las recomendaciones del Comité de Ministros del Consejo de Europa de 1973 y 1974, sobre la creación de bancos de datos en el sector privado y público, respectivamente, c) En Septiembre de 1980, la Recomendación de la OCDE, sobre el flujo internacional de datos, protección a la intimidad y las libertades fundamentales, d) Recomendación del 30 de abril de 1980, relativa a la enseñanza, la investigación y la formación en materia de “informática y derecho”, e) La Recomendación del 18 de septiembre de 1980, relativa al intercambio de informaciones jurídicas en materia de protección de datos, f) La Recomendación del 23 de enero de 1981, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados, g) La Recomendación del 23 de Septiembre de 1983, relativa a la protección de los bancos de datos de carácter personal utilizados con fines de investigación científica y de estadísticas, h) La Recomendación de 23 de enero de 1986, relativa a la protección de los datos de carácter personal utilizados con fines de seguridad social”.

Con base en éstos o por inspiración de aquellos, algunos Estados Europeos expidieron sus propias normas de ámbito nacional, relativas al tratamiento

informatizado de datos, con marcadas diferencias tanto en la conceptualización de los términos técnico-jurídicos (datos, fichero, banco de datos, tratamiento "automatizado", etc), como en lo referente a la enunciación y enumeración de principios, derechos, deberes y excepciones al tratamiento y la protección de los datos, lo cual indicaba que

---

(149) Vid., RIASCOS GOMEZ, Libardo O. *LOS DENOMINADOS RECURSOS ANTE LOS TRIBUNALES DE JUSTICIA DE LA C.E. Y ANDINO.* Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, pág. iii y 1 a 3.

(150) DAVARA RODRIGUEZ. Miguel A. *MANUAL DE DERECHO INFORMATICO.* Ed. Aranzadi S.A., Pamplona (Nav.), 1997, pág. 56-61.

no existía univocidad en los temas referidos, en el grado y categorías de protección que estilaban dispensar a los datos de carácter personal sometidos a tratamiento informatizado en uno y otro país, ni menos el ámbito de los derechos fundamentales que en éste se involucraban si no era únicamente el de la intimidad.

Orti Vallejo [**151**] , estima que esta etapa de legislación estatal de protección de datos, se caracteriza por la preocupación de tutelar la intimidad de la persona, como lo acredita el hecho de que se protejan las informaciones consideradas sensibles, que son aquellas que tienen una más inmediata incidencia sobre la vida privada y sobre el ejercicio de las libertades. Cierto es que esta etapa, también se comienza a introducir una mayor libertad en la creación de ficheros de datos personales, pero, como contrapartida, se otorgan más garantías al derecho de las personas a conocer sus datos contenidos en ficheros o banco de datos mediante el derecho de acceso y consecuentemente a rectificar o cancelar informaciones inexactas o indebidamente procesadas. Sin embargo, como hemos visto y abundaremos sobre ello, esta época legislativa de protección de datos produjo dos enclaves actualmente vigentes: por un lado, el matrimonio de las leyes de protección de datos aparentemente únicamente con el derecho a la intimidad, produjo a partir de ésta época una identificación casi plena sustentada en la argumentación de que la informática atentaba directa y plenamente a la intimidad y no al conjunto de derechos y libertades fundamentales, tal como se revelaría en las diversas normas protectoras de datos personales; y por otro lado, considerar al derecho de *habeas data* como una sola emanación del derecho anglosajón del *habeas corpus* y de aplicación exclusiva al tratamiento de la información manual o mecanizada, sino también, a todo procedimiento de tratamiento de datos personales de carácter informatizada. Esto replanteaba el tradicional de "derecho de acceso" a la

información que tiene toda persona sobre los datos que le conciernen, así como los facultades subsecuentes, de conocimiento, consulta, rectificación, bloqueo y cancelación de información o datos personales que sean erróneos, inexactos o ilegales

De ésta época, tomaremos como prototipo de análisis y estudio las normas supraestatales o comunitarias de protección de datos personales que tendieron desde aquella época hasta los actuales momentos por la normatización y normalización del

---

(151) ORTI VALLEJO. A. Ob. ut supra cit., pág. 15

tratamiento informático de datos personales, la protección integral de los derechos, libertades públicas (o "individuales") e intereses legítimos. En efecto, abordaremos la Recomendación del Consejo de la OCDE, del 23 de Septiembre de 1980, cuyo ámbito se extiende a los Estados de la Comunidad Europea (hoy, UE) y los algunos Estados de Oriente y Occidente. Así mismo. En efecto, el Convenio de Estrasburgo de 28 de Enero de 1981, el cual creo un espíritu normalizador de todo cuanto existía en Europa sobre tratamiento informatizado de datos personales.

4.3.1. LA RECOMENDACIÓN DEL CONSEJO DE LA OCDE, DE SEPTIEMBRE DE 1980

La OCDE (Organización de Cooperación y Desarrollo Económico), creada en 1948, como organización de cooperación preferentemente económica entre Estados Europeos que hoy forman la UE (Unión Europea), EE.UU y Canadá (1960), Japón (1964), Finlandia (1969), Australia (1971) y Nueva Zelandia (1973). Sin embargo, las funciones de esta organización internacional de Estados también se dirige desde su nacimiento hasta la actualidad a proyectar, planear, desarrollar, emitir conceptos, sugerencias y recomendaciones sobre diferentes aspectos de la vida que inciden de alguna manera en lo económico, tales como las estrategias, políticas y directrices sobre la protección de derechos fundamentales, libertades públicas e intereses legítimos de las personas naturales, jurídicas, públicas o privadas, según fuere el caso, con miras esencialmente ha facilitar la armonización de las legislaciones nacionales de los diferentes Estados que componen la OCDE.

En éste último orden de ideas, la OCDE recomendó a sus Estados Miembros, sin perjuicio de sus legislaciones internas sobre la materia [152], unas directrices sobre la

(152) El artículo 5 del Convenio de 14 de diciembre de 1969, de la OCDE, expresa: "Con miras a alcanzar sus objetivos, la Organización, podrá: a) adoptar decisiones que, salvo disposición en contrario, vincularan a todos los miembros: b) formular recomendaciones a los miembros; c) concertar acuerdos con sus miembros, con Estados no miembros y con organizaciones internacionales". Por su parte, el articulo 18 del Reglamento de Procedimiento de la OCDE, de julio de 1976, dispone: "a) Las decisiones de la Organización, adoptadas de conformidad en los artículos 5, 6 y 7 del Convenio, podrán ser: (i) decisiones obligatorias para sus miembros, y que estos ejecutarán previo cumplimiento de los procedimientos que requieren sus constituciones; (ii) decisiones por las que fueren aprobados acuerdos concertados con sus miembros, con Estados no miembros y con organizaciones internacionales; (iii) decisiones de orden interno relativas al funcionamiento de la Organización, que se denominaran resoluciones; (iv) decisiones por las que se hicieren comunicaciones a Estados no miembros o a organizaciones. b) *Las Recomendaciones* de la Organización, formuladas de conformidad con lo dispuesto en los artículos 5, 6 y 7 del Convenio, serán sometidas a la consideración de los miembros para que estos procedan a su ejecución si lo estimaren oportuno, c) los textos de las Decisiones o de las Recomendaciones a que se alude en los apartados a), (i) y b) que anteceden, deberán incluir una referencia al articulo 4- a) o al articulo 5-b), respectivamente". Citado por RIVERA LLANO, A. Ob.cit.,p.178.

protección de derechos fundamentales, como el de la intimidad, las “libertades individuales”, y sobre todo el derecho a la información que tiene toda persona y “conciliar valores fundamentales aunque susceptibles de entrar en conflicto, tales como la intimidad y el libre flujo de la información” (Preámbulo del Convenio). Esta recomendación previos los proyectos y estudios, por parte de las comisiones y subcomisiones de expertos respectivas se concretó en lo que se conoce como “Recomendación Adoptada por el Consejo de la OCDE (con base en los arts. 1 (c), 3 (a) y 5 (b) del Convenio relativo a la OCDE, de 14 de diciembre de 1960) del 23 de Septiembre de 1980, *“por la que se formulan directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales”*.

El Texto de la Recomendación propuesto al Consejo por el Comité de Política Científica y Tecnológica, fue aceptado por los Estados Miembros de la OCDE, entre los que Estaba España, Alemania Occidental, Austria, Bélgica, Dinamarca, EE.UU., Finlandia, Francia, Grecia, Italia, Japón, Luxemburgo, Noruega, Nueva Zelandia, los Países Bajos, Portugal, Suecia y Suiza; en tanto que, Islandia, Turquía y el Reino Unido adhirieron a la Recomendación, el 21 de enero de 1981 y el 27 de Octubre de 1981, respectivamente, no sin mantener su abstención por lo que se había sostenido en la sesión de 23 de Septiembre de 1980.

La Recomendación de la OCDE, constituye un documento de capital importancia para aquella época e incluso con plenas y claras incidencias en la

actualidad, tanto en las legislaciones internacionales como en las comunitarias europeas [153]. El documento preparado por un grupo heterogéneo de expertos de diferentes Estados de Occidente y Oriente del mundo, es un fiel, serio, oportuno y claro diagnóstico y recetario de los innumerables hechos, sucesos, problemas, conflictos y proposición de sugerencias y soluciones a los mismos, sobre todo lo atinente al *flujo internacional de datos* entre países miembros de la OCDE y la protección de los derechos fundamentales como el de la intimidad (aunque no en todo su contexto, pues sólo se destaca la visión iusinformática de la intimidad), como hace énfasis el preámbulo, el texto y contexto y las Memorias Explicativas (en adelante M.E.) de la

---

(153) El profesor destaca esa importancia de la Recomendación de la OCDE, pero más dirigida a la vocación legislativa de los Estados Miembros que con vocación europeísta, y más aún, internacionalista, tal y como fue su origen y presentación. DAVARA RODRIGUEZ, Miguel. *MANUAL DE DERECHO INFORMATICO...* Ob.cit., pág. 57.

Recomendación; además del conjunto de las llamadas *libertades individuales* (surgidas en la historia del constitucionalismo del liberalismo anglo-francés, y que hoy se consideran como un ámbito importante de los derechos fundamentales) [154], dentro de las cuales se encuentra el hoy llamado "derecho de habeas data", el derecho a la información y los derecho de impugnación y recurso que tiene toda persona contra decisiones administrativas o judiciales.

La Recomendación de la OCDE, en el anexo correspondiente a las " *directrices sobre protección de la intimidad y de los flujos de datos de carácter personal a través de las fronteras"*, estructura las cinco partes en las que se compone. Estas están referidas a las generalidades, Los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales aplicables en el ámbito internacional: libre circulación y restricciones legítimas, la aplicación de los principios en el ámbito interno; y, la cooperación internacional.

A nuestros efectos destacaremos, los siguientes temas: a) las definiciones en el tratamiento informatizado de los datos personales y, b) los principios y excepciones fundamentales del tratamiento informatizado de los datos, tanto en el ámbito nacional como en el ámbito internacional, y dentro de éste especialmente, el principio denominado de la *libre circulación de datos personales* y las restricciones legítimas.

---

(154) La importancia mundial que han adquirido los derechos fundamentales en el ámbito del derecho constitucional español a tenido relevancia muchísimo antes del reconocimiento constitucional en 1978, tal y como lo sostiene *SEMPERE*, al referirse a la "Tutela constitucional de los derechos fundamentales de la personalidad", y en especial *al derecho a la intimidad* prevista en el art. 18 CE, que en el momento de la entrada en vigor del texto constitucional ya existía un cuerpo consolidado de doctrina y jurisprudencia con el reconocimiento y tutela de los derechos del honor, la intimidad, la imagen; entre otros. En igual forma, se suma a ello, que con carácter preconstitucional la protección de los derechos fundamentales, tanto en el ámbito penal (doctrina del T.C., sobre los delitos de injurias y animus iniuriandi y una nueva regulación del C.P.) como en el ámbito de la tutela civil (L.O.1/1982, de 5 de Mayo), así como en relación con la compatibilidad de uno u otro tipo de tutela y la posibilidad de elección, entre ellos, por el interesado. Tal reconocimiento determina, al menos, cuatro consecuencias a destacar: 1. El reconocimiento de los derechos privados de la personalidad mencionados en el artículo 18 como derechos fundamentales. El mismo conlleva una doble consecuencia. Por un lado, afirmar que ya no tiene mucho sentido hablar de estos derec*hos como derechos subj*etivos de naturaleza privada, sino como derechos fundamentales de la personalidad, tal como lo sostiene *DIEZ PICAZO*. Por otro lado, en el ejercicio y limitaciones de estos derechos debe aplicarse la doctrina del T.C., sobre los derechos fundamentales. 2. Exigencia de garantía frente al legislador ordinario. Se concretaría en el respeto por parte de las leyes que reg*ulen el ejercicio* de estos derechos, de un contenido mínimo esencial (art. 53.1 CE). Concepto éste jurídicamente indeterminado cuyo control corresponde, en últ*imo término, al TC (a*rt.12), a través del recurso de inconstitucionalidad, recurso con el que se garantiza la primacía de la C.E. --arts. 161.1. a) CE y 27 y 55.2 de la L.O.T.C. 3. *Cualificación de la interven*ción del legislador: reserva de la ley orgánica. Implica que la ley que desarrolle el ejercicio de estos derechos, tanto en su aprobación como modificación, se ajuste a un procedimiento y quórum especiales (art. 168 CE), dado que se trata de leyes orgánicas (art. 81 y 82 CE). 4 . Habilitación de tutela especial ante el Tribunal Constitucional: Recurso de amparo.... SEMPERE RODRIGUEZ, Césa*r. ARTICULO 18: DERECHO AL HONOR,* A LA INTIMIDAD Y A LA IMAGEN. En: COMENTARIOS A LA CONSTITUCION. Ob.ut supra cit.págs..390 y ss.

4.3.1.1. DEFINICIONES BASICAS EN EL TRATAMIENTO INFORMATIZADO DE LOS DATOS PERSONALES

Siguiendo el criterio --generalizado en la década de los ochenta-- la Recomendación de la OCDE, prevé una serie de definiciones iusinformáticas, tales como, Responsable del fichero, datos de carácter personal y flujos internacionales de datos de carácter personal. Se abstiene de definir lo que debe entenderse como "tratamiento automático de datos", pese a que en el preámbulo y en el apartado tercero referido a los "grados de sensibilidad de los datos", se menciona expresamente. Las razones, entre muchas otras, son: limitar al máximo las definiciones; y en el caso específico, porque resulta difícil hacer una distinción clara entre tratamiento "automático y no automático de la información" **[155]** y porque las directrices no están dirigidas exclusivamente al tratamiento de datos de carácter personal con "ordenadores" (o "automático"), aunque curiosamente esto fue la punta del iceberg que convocó la reunión, estudio y planteamiento de las recomendaciones ahora comentadas **[156]**.

La persona física a la que se refiere la definición tiene que gozar de una habilitación legal para decidir, sobre el contenido y utilización de los datos, independientemente de si los datos han sido o no obtenidos, registrados, tratados o

difundidos por dicha persona o por una persona que obra en su nombre. El responsable del fichero puede ser una persona física o jurídica, una autoridad u orga-

---

(155) Cfr. MEMORIA EXPLICATIVA (M.E) Punto 34. "*Tratamiento automático y no automático de datos"*. Las actividades que la OCDE había venido dedicando a la protección de la intimidad y a otros ámbitos conexos estaban centradas en el tratamiento automático de la información y en las redes de ordenadores. El grupo de expertos considero con especial atención la cuestión de si el alcance de estas directrices debía o no quedar limitado al tratamiento automático e informatizado de los datos de carácter personal. Este enfoque puede justificarse por razones diversas, tales como los especiales peligros que llevan consigo para las libertades individuales la automatización y los banco de datos informatizados, el creciente predominio de los métodos de tratamiento automático de la información, en especial en el contexto de los flujos internacionales de datos, así como el marco especifico de la política de la información, de la informática y las comunicaciones, dentro del cual hubo de cumplir su mandato el grupo de expertos. AA.VV. *DOCUMENTACION INFORMATICA.* Serie Amarilla.Tratados Internacionales núm. 2.

(156) M.E. Punto 35. "Así, por ejemplo, existen sistemas mixtos de tratamiento de la información y hay también ciertas etapas del tratamiento de la información que pueden o no ser susceptibles de automatización. Estas dificultades pueden agravarse aun mas como consecuencia de los continuos progresos técnicos, tales como la aparición de métodos semiautomáticos perfeccionados basados en la utilización de microfilmes o de microordenadores, que podrán ser empleados cada vez más para fines meramente privados, a la vez inofensivos e incontrolables. A mayor abundamiento, si las directrices se centraran únicamente en los ordenadores podrían dar lugar a incoherencias y lagunas, del mismo modo que podrían crear para los responsables de ficheros posibilidades de obviar las normas de aplicación de la directrices con sólo utilizar medios no automáticos para fines que podrían ser nocivos". Ibídem Ob. ut supra cit.

nismo público.

La definición excluye, por tanto a: a) las autoridades competentes para conocer autorizaciones o licencias y los organismos que autorizan el tratamiento de la información pero son competentes para decidir sobre que actividades deben llevarse a cabo y para que fines; b) las empresas de servicios informáticos que realizan actividades de tratamiento de la información por cuenta de terceros; c) las autoridades competentes en materia de telecomunicaciones y los organismos análogos; d) los *usuarios dependientes*, que si bien pueden acceder a los datos, no están sin embargo autorizados para decidir sobre que datos deberían ser registrados o cuales utilizados (M.E. núm.40).

Los *Datos de carácter personal*, o simplemente datos personales, se considera cualquier información relativa a una persona física identificada o identificable --o también interesado-- (R.1-b). Las directivas se aplicarán tanto a los datos personales en el sector público como en el sector privado, siempre que acarrearen un peligro para la intimidad y las libertades individuales, a causa de la manera en que fueren elaborados o por razón de su naturaleza o del contexto en que fueren usados (R.2). En esta aplicación deberá observarse: a) las medidas de

protección a las diversas clases de datos tanto en la obtención, almacenamiento, elaboración o difusión. b) que no se excluyen ni siquiera datos de carácter personal que de manera manifiesta no ofrecieren riesgo alguno para la intimidad y las libertades individuales [157], y c) que no se limitará la aplicación de las directrices a la "elaboración automática" de datos personales (R.3).

Los *flujos internacionales de datos de carácter personal,* se consideran a los movimientos de datos de carácter personal a través de las fronteras nacionales (R.1-c).

Aunque hace referencia a los flujos internacionales, las directrices no tienen en cuenta problemas hacia el interior de los Estados Federales. Los movimientos de datos

---

(157) M.E. Punto 1 a 3. Los problemas prioritario que detectaron las comisiones y subcomisiones de expertos se refieren principalmente al derecho a la intimidad; la informática, la tecnología (de ordenadores, redes de comunicación), las telecomunicaciones, el derecho a la información y el de "habeas data", aunque en el texto de la Recomendación y las M.E., se hace mención genérica al derecho de acceso a la información, a conocer, actualizar, cancelar o modificar los datos de carácter personal por el titular o interesado; el "tratamiento automático de la información. En particular se refieren a la intimidad en un concepto más amplio que el tradicional derecho de "sólo dejar a solas" -- el "The Right to Privacy" anglosajón--, y algo que se convertirá en la cantinela de proposición de toda la Recomendación, al decir: "con la expresión intimidad y libertades individuales constituye el aspecto más controvertido" de todos cuantos se tratan en la Recomendación de la OCDE de 1980.

tendrán lugar a menudo mediante la transmisión electrónica, pero también pueden servirse de otros medios de transmisión, así como por vía satélite (M.E.núm. 42).

4.3.1.2. PRINCIPIOS Y EXCEPCIONES FUNDAMENTALES DEL TRATAMIENTO INFORMATIZADO O NO DE LOS DATOS PERSONALES.

Las partes segunda, tercera y cuarta de la Recomendación de la OCDE, se destinan a hacer referencia a los principios fundamentales a aplicar en el ámbito interno, los principios fundamentales a aplicar en el ámbito internacional: libre circulación de los datos y restricciones legítimas y aplicación de los principios en el ámbito interno, que no es más que un aparte reiterativo de las gestiones administrativas, jurídicas, legislativas "y de otra índole" que los Estados Miembros de la OCDE deben adelantar para implementar los medios y mecanismos idóneos para aplicar los principios en sus ámbitos legislativos internos y hacer efectivas las medidas de protección del derecho a la intimidad y las libertades individuales [158].

Los principios fundamentales aplicables al tratamiento informatizado o no de los datos personales en el ámbito nacional, según la directiva son: a) limitación de la colecta de los datos, b) calidad de los datos, c) especificación del fin, d) restricción del uso, e) garantía de la seguridad, f) transparencia, g) participación del individuo y h) responsabilidad.

En el plano internacional, los principios básicos aplicables al tratamiento (infor- matizado o no) de los datos personales, constituyen un complejo grupo de principios y límites que estructuran a su vez, el principio fundamental denominado: *libre circulación de datos personales* dentro de un flujo o movimiento internacional de los mismos.

---

(158) P.IV: "*APLICACION DE LOS PRINCIPIOS EN EL AMBITO INTERNO*. 19. Los países miembros al aplicar en su ámbito interno los principios (parte II y III) deberán crear mecanismos jurídicos, administrativos y de otra índole, o instituciones, tendentes a proteger la intimidad y las libertades individuales con respecto a los datos de carácter personal. En especial, los países miembros deberán: a) promulgar una legislación interna idónea, b) fomentar y apoyar las reglamentaciones autónomas, bien en forma de códigos de deontología, bien en otra forma, c) poner a disposición de las personas físicas medios idóneos para ejercer sus derechos, d) instaurar sanciones y recursos para los supuestos de inobservancia de medidas de aplicación de los principios que se detallan en las partes II y III. e) velar porque no exista discriminación desleal alguna contra los interesados".

4.3.1.2.1. PRINCIPIOS DEL TRATAMIENTO DE DATOS EN EL AMBITO NACIONAL.

Aunque se hace una distinción de los principios tanto en el ámbito nacional y el ámbito internacional, y dentro del primero en cada una de las fases del tratamiento de los datos personales (recolección, almacenamiento, registro, difusión y flujo), lo cierto es que dichos "principios son interdependientes y en parte se entrecruzan y traslapan. Por ello, las distinciones que con relación a los principios se hacen entre las actividades y las fases del tratamiento de datos son artificiales y no deben impedir que los principios sean tratados conjuntamente y estudiados como un todo" (M.E.50). Esto se evidenció además, al analizar que los diferentes Estados Miembros de la OCDE, en sus diferentes iniciativas legislativas internas para la protección de la intimidad y las libertades individuales tienen muchos rasgos comunes, así como intereses, valores básicos y principios fundamentales **[159]** que guían y orientan las fases o ciclos del tratamiento de los datos personales.

Analicemos brevemente los mencionados principios:

1. El *Principio de limitación de la colecta de datos*, hace referencia a aquellos datos personales que, debiendo ser obtenidos por medios legítimos y leales, y en el caso en que fuere procedente, con el conocimiento o el consentimiento del interesado, dichas actividades deberán ser limitadas (R.7).

Este principio hace referencia a dos aspectos: a) los limites que han de fijarse a la colecta de aquellos datos que debieren ser considerados como especialmente dato

---

(159) Esos rasgos comunes se sintetizan así: a) "poner límites a la colecta de datos personales, de conformidad con los objetivos del que hace acopio de tales datos y con otros criterios", b) "restringir el uso de los datos, de tal forma que se acomode a unos fines claramente expuestos; c) adoptar los medios necesarios para que el individuo conozca la existencia y el contenido de los datos y pueda requerir la corrección de los datos, y d) determinar las personas responsables del cumplimiento de las disposiciones y resoluciones de protección de la intimidad y de las libertades individuales que fueren aplicables. "En términos generales, las leyes de protección de la intimidad y de las libertades individuales con relación a los datos de carácter personal tienden a cubrir las sucesivas etapas del ciclo que comienza con la colecta inicial de los datos y termina con la cancelación u otras medidas semejantes, y a garantizar en lo posible el conocimiento, participación y control del individuo con respecto a dicho ciclo". M.E. núm. 5.

sensibles **[16 0]** a causa de la manera en que hubieren de ser tratados, su naturaleza, el contexto en el cual hubieren de ser utilizados, y b) las condiciones que deben cumplir los métodos de colecta de datos.

En cuanto al primer aspecto, hay que resaltar lo siguiente: Se deberá poner fin a la colecta indiscriminada de datos personales, y más aún cuando se trata de universalizar la consideración de qué datos se consideran sensibles. Para esto, la Recomendación suministra una serie de pautas que sirvan para determinar la índole de tales límites. Estas son: a) los aspectos cualitativos de los datos (es decir, que deberá ser posible extraer de los datos obtenidos una información de una calidad suficientemente buena, y que los datos deberán ser obtenidos dentro de un marco informativo apropiado); b) la finalidad del tratamiento de la información (es decir, que sólo deberán ser obtenidos determinados datos y, a ser posible la colecta de datos se limitará al mínimo necesario para lograr la finalidad prevista): (i) Identificación mediante "marcas" de aquellos datos que según las tradiciones y actitudes propias de cada país miembro fueren especialmente sensibles; (ii)

actividades de colecta de datos de determinados responsables de datos; (iii) preocupaciones relativas a los derechos humanos (M.E. núm. 51).

En cuanto al segundo aspecto, es decir las condiciones de los métodos de colecta de datos, se advierte contra ciertas prácticas que implican, por ejemplo, el uso de dispositivos ocultos de registro de datos, tales como magnetófonos u otros que inducen a error a los interesados, moviendoles a facilitar información. La necesidad de poner los datos en conocimiento del interesado (que puede estar representado por un tercero, como en el caso de los menores de edad o personas "deficientes mentales"…)

---

(160) Dado que por aquel entonces y hasta ahora, determinar el "grado de sensibilidad de los datos" resulta un labor titánica, aún cuando se acude a circunstancias específicas de potencialidad del riesgo, se consideró por los expertos de la Recomendación de la OCDE, hacer mención genérica de los "datos sensibles" para que sean los Estados Miembros quienes determinen cuáles se pueden considerar como tales. Se hacía mención por ejemplo, que mientras en unos países los "identificadores personales universales" (tarjeta de identidad o cédula de ciudadanía, número de identificación profesional, de seguros, etc.), se consideran inocuos y útiles; en otros, se consideran algo delicado. Así mismo, se puso en evidencia, la disparidad de las legislaciones sobre qué datos se consideran o no sensibles. En efecto, en "las legislaciones europeas existen precedentes al respecto --es decir, considerar datos sensibles a los datos referidos a la-- (raza, creencias, religiosas, registros de condenas, p.e.). Pero también se puede argüir que ningún dato es intrínsecamente privado o sensible, sino que puede llegar a serlo según su contexto y el uso que del mismo se haga. Esta opinión se refleja en la legislación de los Estados Unidos de protección de la intimidad, por ejemplo.(M. E. 50). En las partes III y IV., de esta investigación volveremos sobre el tema.

o de obtener su consentimiento para registrarlos, constituye una norma básica, y el conocimiento, la exigencia mínima. Sin embargo, por razones prácticas, no es posible siempre exigir el consentimiento. p.e. las investigaciones criminales y la actualización periódica de las listas de distribución de correspondencia (M.E. núm. 52).

2. El *Principio de calidad de los datos*. Los datos personales deben ser pertinentes con respecto a los fines para los que fueron usados, y, en la medida en que fueren necesarios para tales fines, deberán ser exactos y completos, debiendo asimismo ser actualizados constantemente (R.8) .

La calidad de los datos hace relación a dos aspectos claramente definidos para toda información, más cuando ésta es de carácter personal. En efecto; uno, es el cumplimiento en todo el tratamiento (informatizado o no) de datos desde la recolección misma hasta la fase de difusión, recuperación o transmisión acerca de la finalidad con que han sido tratados los datos y su correspondiente utilización

posterior; y otro, como verificación de lo anterior, el de que los datos tratados deberán ser exactos, completos y constantemente actualizados. Estos aspectos están interrelacionados, puesto que no se puede exceder en la utilización de los datos la finalidad para las cuales fueron tratados (informatizada o no) en su momento. v.gr. En los datos relativos a opiniones pueden fácilmente inducir a error si se utilizan para fines con los cuales no guardan relación alguna. Lo mismo puede decirse con respecto a los datos valorativos.

Sin embargo, se evidencia que en alguna clase de datos personales el criterio de la finalidad, lleva consigo el problema de si se puede o no causarse perjuicio a los interesados por falta de exactitud, de completud y de actualidad. Tal sería, el caso de las investigaciones de las ciencias sociales que llevan aparejados los llamados estudios "longitudinales" de la evolución de la sociedad, de investigaciones históricas y de actividades de archivo (M.E.núm. 53).

3. El *Principio de especificación del fin.* Los fines para los cuales se obtuvieren datos personales deberán ser precisados en el momento de la colecta de datos, debiendo su subsiguientemente uso limitarse al cumplimiento de tales fines o de aquellos otros que, sin ser incompatibles con los mismos, fueren especificados cada vez que fueren modificados (R.9).

Este principio reitera, complementa y concreta el anterior principio, poniendo énfasis en la relación utilización y finalidades previstas para el tratamiento (informatizado o no) de datos, los cuales deben precisarse desde el momento mismo de la recolección.

Los fines pueden ser definidos de maneras diversas y complementarias, principalmente por medio de declaraciones públicas, o bien informando a los interesados, por medio de la legislación, resoluciones administrativas y autorizaciones otorgadas por los organismos de tutela.

Así, cuando los datos hubieren dejado de estar subordinados a un fin y, siempre que fuere posible, podrá ser necesario hacerlos destruir (borrar) o darles forma anónima. Esto por cuanto, los datos dejan de tener interés, sucede que se

pierde el control sobre ellos y pueden surgir nuevos riesgos, tales como, “el hurto, reproducción no autorizada o de otras acciones ilícitas” (M.E.núm. 54 *in fine*) .

4. El *Principio de restricción del uso*. Los datos personales deberán ser revelados, facilitados o, en general, usados para fines que no fueren los que se especificaren de conformidad con el anterior principio, excepto en los siguientes supuestos: a) previo el consentimiento del interesado, b) previa habilitación legal al efecto (R.10).

Este principio que limita el uso de los datos en ciertos y precisos casos, no es más que un principio bisagra de los principios relativos a la calidad y la determinación del fin, y como tal, juega un papel de inmovilizador de las facultades discrecionales que tuvieran las autoridades competentes, responsables de un fichero o incluso usuarios de los datos personales tanto en la revelación o divulgación como en el mera uso de los mismos. Por ello, se limita la divulgación o el uso de los datos que impliquen desviaciones con respecto a las finalidades previamente determinadas

La regla general, por la cual todo tratamiento de datos debe tener previamente determinadas sus finalidades desde el momento mismo de la recolección, precisa dos excepciones, a saber: una, por el consentimiento del interesado (o de su representante, en el caso de menores, etc.); y otra, por disposición normativa. Estas excepciones son *numerus clausus*, y por tanto, no cabe excepciones interpretativas según este principio.

En tal virtud, podría destinarse datos personales a fines de investigación, estadísticos y de planificación social, que inicialmente se han obtenido con miras a tomar decisiones de tipo administrativo, sin que media para ello, el consentimiento o así lo determine una norma jurídica.

5. El *Principio de garantía de la seguridad*. Deberán preverse medidas adecuadas de seguridad para proteger datos personales contra riesgos tales como la pérdida o el acceso, destrucción, uso, modificación o divulgación de los mismos sin la oportuna autorización (R.11).

Este principio constituye el epicentro de las medidas de protección del derecho a la intimidad y de las libertades individuales, cuando se ha sometido a

tratamiento (informatizado o no) datos personales por quienes están involucrados en dicho tratamiento. Para concretar las denominadas “garantías adecuadas”, contra los riesgos tales como, la pérdida de datos (que incluye el borrado a causa de accidente, la destrucción de soportes de información y el “hurto” de tales soportes), el acceso no autorizado para destruir, modificar o divulgar datos, o más aún, el uso indebido o no autorizado de los mismos (que incluye la reproducción no autorizada de datos), deberán las autoridades competentes implementar medidas idóneas proporcionales a los riesgos que los titulares de los datos pueden sufrir.

El grupo de expertos de la Recomendación de la OCDE, a título de ejemplo, propuso una serie de “garantías adecuadas”, tales como, las de índole material (cerrojos en puertas y tarjetas de identificación, por ejemplo), *medidas de organización* (niveles jerárquicos en relación con el acceso a los datos, así como la obligación que tiene el personal responsable del tratamiento de la información de *respectar el carácter confidencial de los datos*), y sobre todo en los sistemas informáticos, *medidas relacionadas con la información* (encriptación, control de actividades inusitadas capaces de constituir un peligro y medidas tendentes a hacerles frente). (M.E. núm. 56).

6. El *Principio de transparencia*. Deberá adoptarse una norma general de transparencia en cuanto a las innovaciones, prácticas y criterios existentes con respecto a los datos personales. Deberá ser posible disponer fácilmente de medios que permitan determinar la existencia y naturaleza de los datos personales, el fin principal de su uso y la identidad del responsable de los datos y la sede habitual de sus actividades (R.12).

Como lo expone el grupo de expertos de la OCDE, el principio de transparencia puede ser considerado como condición previa del principio de participación individual. Como tal se considera una condición *sine qua nom*, para que pueda darse cabal y recto cumplimiento a uno de los principales principios con relación al tratamiento de datos, cual es el de la participación individual.

7. El *Principio de participación del individuo*. Toda persona física gozará de los siguientes derechos: 1) obtener del responsable del fichero o de otra instancia la confirmación de si el responsable de datos tiene datos acerca de su persona. 2)

Requerir que se le comuniquen los datos que hicieren referencia a la misma, y ello: i) dentro de un plazo prudencial, ii) previo abono, en su caso, de una tasa que no fuere excesiva, iii) de manera razonable, iv) de manera directamente inteligible. 3) ser informado de la motivación de la resolución denegatoria de la petición formulada al amparo de los apartados *a*, y *b*, y poder recurrir contra la denegación. 4) impugnar datos que hicieren referencia a la misma y, en el supuesto de que la impugnación fuere fundada, requerir que los datos fueran cancelados, rectificados, completados o modificados (R.13).

Este principio fundamental esta estructurado por una serie de derechos y deberes que tienen y deben cumplir los sujetos interactuantes en el tratamiento o procedimiento (informatizado o no) de la información o datos. En efecto, se establecen los derechos que goza toda persona física en el transcurso del tratamiento de datos desde la recolección misma, así como las obligaciones que tienen que cumplir los responsables del fichero o autoridades competentes para proteger, respetar y hacer respetar esos derechos. Todo ello, dirigido a garantizar la protección de la intimidad y las libertades individuales.

Cuando en el principio se hace mención a los derechos que tiene toda persona para acceder, conocer, impugnar, y en su caso solicitar, la cancelación, rectificación, complementación o modificación y actualización de los datos personales que le conciernen, simple y llanamente estamos haciendo referencia al derecho denominado de "*habeas data*", por el cual la persona puede tener control de sus propios datos. Obviamente este derecho, como todo derecho fundamental, no es absoluto y está sometido a limitaciones previstas en las propias normas jurídicas.

Por ello, los expertos de la OCDE, concretaron lo siguiente:

a) El derecho de acceso deberá ser, en general, fácil de ejercitar. Esto puede significar, entre otras cosas, que debería formar parte del conjunto de las actividades cotidianas del responsable del fichero o del que hiciere sus veces y no requerir proceso judicial o medida análoga alguna. En algunos casos podría quizá ser conveniente prever un acceso intermedio a los datos; así, por ejemplo, en la esfera médica el médico podrá servir de intermediario.

b) La condición de que los datos sean comunicados dentro de un plazo razonable puede ser cumplida de modos diversos. Así, el responsable de un fichero que facilite información a los interesados a intervalos regulares puede ser dispensado de la obligación de responder inmediatamente a las peticiones formuladas individualmente. Normalmente, el plazo deberá ser computado desde la recepción de una petición. Su duración podrá variar en cierta amplitud de una situación a otra en función de circunstancias tales como la índole del tratamiento de la información.

c) La comunicación de tales datos *de manera razonable* significa, entre otras cosas, que debe presentarse la debida atención a los problemas de la distancia geográfica, cuando menos.

d) El derecho a ser informado de las razones, en los términos previstos en el apartado 3, es limitado en cuanto que se constriñe a situaciones en las cuales hubieren sido desestimadas peticiones de información.

e) El derecho a impugnar, contemplados en los apartados 3 y 4, tiene una gran amplitud, y comprende las reclamaciones formuladas en primera instancia ante los responsables de los datos y asimismo los subsiguientes recursos presentados ante tribunales, organismos administrativos, órganos profesionales u otras instituciones, siguiendo los cauces previstos en los reglamentos internos de procedimiento. El derecho a impugnar no implica que el interesado pueda decidir cuáles sean los recursos o reparaciones disponibles (rectificación, incluso de una anotación que precise que los datos son objeto de litigio, etc.); tales cuestiones serán resueltas aplicando el Derecho interno y los cauces procesales internos (M.E. núms. 58 a 61).

8. El *Principio de responsabilidad*. El responsable del fichero deberá responder de la observancia de las medidas tendentes a dar cumplimiento a los principios que anteceden (R.14). Este principio dirigido al responsable de los ficheros constituye el principal principio-deber de éste y principio-derecho de los titulares de los datos personales para demandar su efectividad. Este responsable no será dispensado de tales obligaciones ni siquiera cuando el tratamiento de datos es "llevado a cabo por su cuenta por un tercero, como una oficina de servicios, por

ejemplo. Más aún, es probable deducir responsabilidad" al personal de las oficinas de servicios, a los *usuarios dependientes* y a otras personas. Por ello, las sanciones impuestas por incumplir la obligación de *confidencialidad* podrán afectar a todas las personas, físicas o jurídicas, encargadas del tratamiento de los datos de carácter personal (M.E.núm.62).

4.3.1.2.2. PRINCIPIOS DEL TRATAMIENTO DE DATOS EN EL AMBITO INTERNACIONAL: LIBRE CIRCULACION Y RESTRICCIONES LEGITIMAS.

Este grupo de principios que se concreta en el *Principio fundamental de la Libre circulación de los datos*, está previsto en la parte III, apartados 15 a 18 de la Recomendación de la OCDE. Decimos grupo de principios porque la Recomendación no deslinda uno a uno, como sí lo hace en el ámbito nacional, los principios aplicables al ámbito internacional. En los apartados mencionados se dan pautas que unidas concretan el principio fundamental que se quiere resaltar, el de la libre circulación de los datos. Sin embargo, no debemos olvidar que siendo la transferencia, flujo o movimiento de datos uno de los ciclos posibles del tratamiento de datos personales, es lógico pensar que a esta clase de información transmitida en el ámbito internacional se tengan que aplicar los principios generales para todo el tratamiento de la información, es decir, los que hemos comentado en el apartado anterior, para el nivel nacional. Esta tesis se ve reforzada en el texto de la Recomendación misma, pues "los países miembros deberán tender a la formulación de unos principios en el plano interno e internacional que rijan el derecho aplicable en los supuestos de flujos internacionales de datos personales" (R.22), debiendo tener en cuenta estos países "las implicaciones que para otros países miembros tuvieran el tratamiento interno de datos personales y su reexportación" (R.15).

Para conseguir la incardinación de dichos principios e implementar las medidas de seguridad necesarias a nivel internacional, "los países miembros deberán adoptar las medidas razonables oportunas para que los flujos internacionales de datos personales, incluso el tránsito por un país miembro, sean ininterrumpidos y

seguros" (R.16); es decir, que deben estar protegidos contra los accesos desautorizados, la pérdida, destrucción, modificación o cancelación de datos. Esta protección debe extenderse a todos los datos personales, incluso a los "*datos en tránsito*", o sea, aquellos que transitan de un país a otro sin ser utilizados o almacenados en éste con finalidades de posterior uso o consulta [161].

Todo ello, por cuanto a nivel interno, los Estados miembros de la OCDE, presentaban diferentes problemas que no podía resolver aisladamente y surgidos por la adopción de medidas que amparan a la persona con respecto al flujo o movimiento de datos personales a través de sus fronteras [162] . Además porque, este flujo había _____

(161) "EI compromiso general que se contempla en el apartado 16 deberá ser considerado, por lo que respecta a las redes de ordenadores, dentro del contexto del Convenio Internacional de Telecomunicaciones de Málaga-Torremolinos (25 de Octubre de 1973). En virtud de este convenio, los miembros de la Unión internacional de Telecomunicaciones (UIT), entre ellos los países miembros de la OCDE, acordaron entre otras cosas, adoptar las medidas oportunas para crear los canales e instalaciones necesarios con el fin de asegurar un intercambio rápido e ininterrumpido de las telecomunicaciones internacionales. A mayor abundamiento, los países miembros de la UIT acordaron adoptar todas la medidas posibles y compatibles con el sistema de telecomunicación empleado, con objeto de garantizar el secreto de la correspondencia internacional. En cuanto a las excepciones, los miembros se reservaron el derecho de suspender el servicio de las telecomunicaciones internacionales, así como el derecho de comunicar la correspondencia internacional a las autoridades competentes, con el objeto de garantizar la aplicación de su legislación interior o la ejecución de los convenios internacionales en los cuales fueren parte los países miembros de la UIT. Estas normas se aplicarán tan pronto como los datos fueren transmitidos por medio de las lineas de telecomunicación. Dentro de su contexto propio, las directrices constituyen un medio suplementario de garantizar que los flujos internacionales de datos de carácter personal tengan lugar sin interrupción y con plena seguridad" (M.E.núm. 66).

(162) "Otras razones para completar la reglamentación del tratamiento de datos personales a nivel internacional, son: a) los principios en juego hacen referencia a ciertos valores que varios países ansían preservar y ver respetados; b) pueden contribuir a ahorrar gastos en la circulación internacional de datos; c) los países tienen un interés común en evitar la creación de enclaves en los cuales fuera fácil hurtarse al cumplimiento de las reglamentaciones nacionales internas relativas al tratamiento de la información" (M.E.9).

crecido, a la par con la creación de *bancos internacionales de datos* (entendiendo como tales, los conjuntos de datos almacenados para poder ser recuperados y para otros fines). Esto no sólo justificaba la necesidad de cooperación internacional entre los Estados para resolver estos problemas, para velar porque los procedimientos aplicables al flujo internacional de datos personales y la protección de la intimidad y de las libertades individuales sean seguros y compatibles con los de otros países miembros, sino que consecuentemente fundamentaba el *libre flujo de la información*, así como el grupo de principios que éste conlleva, pues hasta ahora la libre circulación de datos " con frecuencia debe ser mitigado en aras de la protección de datos y de las oportunas limitaciones con respecto a su colecta, tratamiento y difusión" (M.E.7).

Se establece como regla general, la libre circulación de los datos personales, como un principio-derecho, no absoluto, y por tanto limitada en los siguientes casos:

a) Todo país miembro deberá abstenerse de restringir los flujos internacionales de datos personales que tuvieren lugar entre su territorio y el de otro país miembro, excepto en el supuesto de que este no observare sustancialmente las presentes directrices o cuando la reexportación de dichos datos permitiere soslayar la aplicación de su legisla- ción interna de protección de la intimidad y de las libertades individuales (R.17 *Ab initio*).

b) Todo país miembro podrá asimismo imponer restricciones con respecto a determinadas clases de datos personales para las cuales su legislación interna de protección de la intimidad y de las libertades individuales previere regulaciones normativas específicas basadas en la naturaleza de tales datos, siempre que el otro país miembro no les otorgare una protección equivalente (R.17 *In fine*). Con ello no se quiere que los países tengan regímenes de protección idénticos (en forma y fondo), sino que sus efectos puedan considerarse en esencia idénticos entre los Estados que intervienen en el movimiento de datos (Emisor/Transmisor de datos. Aunque la Recomendación utiliza una terminología iusmercantilista criticable de Importador/Exportador de datos).

c) Los países miembros deberán abstenerse de dictar disposiciones legales, formular directrices políticas o crear prácticas que, concebidas en nombre de la protección de la intimidad y de las libertades individuales, excedieren las exigencias de dicha protección y fueren por ello incompatibles con la libre circulación de datos personales a través de las fronteras (R.18). Sin embargo, esta restricción impuesta a nivel interno no significa que se limite la actividad legislativa de los Estados sobre flujos transfronterizos en el marco comercial, tarifas aduaneras, empleo y “a otros factores económicos conexos que condicionan el tráfico internacional de datos” (M.E.núm. 68).

4.3.1.2.3. EXCEPCIONES A LAS DIRECTRICES.

La regla general que se establece en la Recomendación para estructurar las excepciones a las Directrices, es la de que éstas constituyen en el ámbito de aplicación de los Estados Miembros de la OCDE, "pautas mínimas susceptibles de ser completadas con medidas adicionales de protección de la intimidad y de las libertades individuales" (R.6).

Si bien, ni técnica ni jurídicamente la Recomendación *sin fuerza ejecutiva*, expone un listado de los supuestos que deben considerarse como excepciones, como se hace en las legislaciones a nivel interno, no debe desdeñarse el hecho de plantear unas pautas generales para su aplicabilidad, partiendo de la expuesta regla general. En efecto, se entiende entonces que las excepciones serán las mínimas posibles y deben darse a conocer al público por medios idóneos (p.e. publicación en diario oficial). Dentro de ese *exceptionis mínimum*, la Recomendación destaca tres supuestos genéricos: La Soberanía y la Seguridad nacionales y el orden público. Aspectos estos que en las diferentes legislaciones de los Estados, aún ahora, han sido definitivos para construir un sistema de excepciones, aún vigente.

El sistema de excepciones propuesto por la Recomendación no fue *númerus clausus* ni concentrado. Lo primero, por lo que se ha dicho anteriormente; y lo segundo, por cuanto no sólo constituyen eventos de excepciones a la regla general del tratamiento (informatizado o no) de datos, ni a la aplicación de los principios que propenden por su protección y garantía, sino porque en el contexto de la Recomendación se exponen supuestos con el nombre de "limitaciones", "restricciones legítimas", etc., que en puridad jurídica constituyen casos de excepciones. Bástenos mirar las llamadas restricciones legítimas al flujo internacional de datos [163].

---

(163) Véase, aparte 4.3.2.12.2.

4.3.2. EL CONVENIO DE ESTRASBURGO DE ENERO 28 DE 1981.

Una armonización legislativa internacional en los Estados Europeos sobre la protección de los datos personales sometidos a tratamiento informatizado por medios idóneos, constituía la aspiración capital del Convenio 108 del Consejo de Europa de 28 de Enero de 1981. Esto es lo que se pretendió con el Convenio de

Estrasburgo, y en efecto se logró. El Convenio Europeo de 1981, como también se le conoce, relativo a la *protección de personas en relación con el tratamiento automatizado de datos de carácter personal*, fue ratificado por España el 27 de Enero de 1984, con lo cual a partir de allí perteneció a los Estados con leyes de protección de datos de la *segunda generación.* Este texto, aparte de constituir norma jurídica de derecho interno en España, por el ingreso al ordenamiento jurídico (art.96.1 CE) y ser un eficaz instrumento de interpretación de los derechos humanos, en lo referente al "uso de la informática" (STC 254/1993, de 20 de Julio), ha servido de modelo normativo (en forma y contenido no muy fiel, como veremos) a la *Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española --LORTAD--*: L.O.5/1992, Oct. 29 **[164]**.

En el Preámbulo del Convenio de Estrasburgo, se establecen las líneas directrices y programáticas para todos los Estados Miembros del Consejo de Europa, así como las posturas jurídicas a observar por los dichos Estados, respecto a la protección de los derechos y libertades fundamentales, en general, y al derecho a la intimidad (aunque conceptualmente se refiera a "la vida privada"), en especial. Esta particularidad ha hecho que la protección en el tratamiento informatizado de datos personales sea inmediatamente identificada en su vulnerabilidad con el derecho a la intimidad, tal como lo hicieran otras normas comunitarias y estatales de protección de datos. Así mismo se confirmó varios postulados y principios previstos en la Recomendación de la OCDE de 1980, pero especialmente sobre la *Libre circulación de datos, la libertad de información y la conciliación y respeto mutuo de derechos y libertades fundamentales.*

Estas Directrices capitales son: a) Propender por una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho

---

(164) Las infidelidades de la LORTAD, hoy son causa de recursos de inconstitucionalidad como veremos al final de esta parte de la investigación. El autor destaca la inspiración de contenido del Convenio seguido por la LORTAD. ORTI VALLEJO. A. Ob. ut supra cit., pág. 17.

así como de los derechos humanos y de las libertades fundamentales; b) Ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; c) Reafirmando al mismo

tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; y d) Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.

Muy a pesar de que el preámbulo en todo cuerpo normativo tiene efectos materiales y jurídicos vinculantes sobre el contexto o articulado, el Convenio prefirió pasar de reiterativo y volvió a plasmar estas directrices en forma resumida en el artículo primero, confirmando con ello la protección en el tratamiento informatizado de datos personales de todos los derechos, libertades públicas e intereses legítimos, no única y exclusivamente el derecho a la intimidad.

El Convenio está dividido en siete capítulos, a saber: 1. *Disposiciones Generales*: Objetivo y fin, definiciones, y ámbito de aplicación; 2. *Principios fundamentales de la protección de datos:* Obligaciones de las partes, calidad de los datos, clases especiales de datos, seguridad de los datos, garantías complementarias para el interesado, excepciones y restricciones, sanciones y recursos, y ampliación de la protección; 3. *De los flujos internacionales*: flujos internacionales de datos de carácter personal y derecho interno; 4. *Del Mutuo Auxilio:*Cooperación entre las partes, asistencia a los interesados residentes en el extranjero, garantías referentes a la asistencia prestada por las autoridades designadas, desestimación de peticiones de asistencia, gastos y tramitación de la asistencia; 5. *Del Comité Consultivo:* Composición del Comité, funciones del Comite, procedimiento; 6. *De las Enmiendas:*Enmiendas; y, 7. *Cláusulas Finales:* Entrada en vigor, adhesión de estados no miembros, cláusula territorial, reservas, denuncia, y notificación.

De este variopinto contenido, abordaremos el análisis de los siguientes temas: a) Las definiciones nucleares en el tratamiento informatizado de datos personales y, b) Los principios y excepciones fundamentales en el tratamiento y circulación de datos .

4.3.2.1. DEFINICIONES NUCLEARES EN EL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES.

El *poder de la informática* desde la expedición del Convenio y mucho antes, hacía gravitar sobre los usuarios de los sectores públicos y privado la consiguiente responsabilidad social. En la sociedad moderna, gran parte de las decisiones que afectan a los individuos descansan en datos registrados en ficheros o

bases de datos (v.gr. Nóminas, expedientes de seguridad social, historiales médicos, judiciales, policiales, etc.). En los años que siguieron a aquella época, el tratamiento informatizado de la información continuó imponiéndose en el ámbito administrativo y de gestión, entre otras cosas, a causa del abaratamiento de los costes del tratamiento informático de los datos, de la aparición en el mercado de dispositivos de tratamiento inteligente y de la creación de nuevos sistemas de telecomunicaciones para la transmisión de los datos, tal como lo destacaba también la Memoria Explicativa del Convenio (M.E.).

Un cierto halo de temor que rondaba a los operadores jurídicos (abogados, jueces, administradores, etc) al aplicar cuerpos normativos jurídico-técnicos, como lo era el Convenio Europeo de 1981, inspiraba a los legisladores a implementar un capítulo preliminar que funcione como glosario técnico-jurídico que guía y orienta a los operadores jurídicos del Convenio. Así, se paliaba ese temor, que aún ahora subsiste en todas las normas que regulan el fenómeno tecnológico de la información y la comunicación (TIC), unido a la informática.

En tal virtud, el Convenio definió los siguientes términos nucleares en todo tratamiento informatizado de los datos: Datos personales, persona identificable, interesado, “fichero automatizado”, “tratamiento automatizado” y “autoridad controladora”, entre otros.

Los datos de carácter personal (o datos personales), se consideran cualquier información relativa a una persona física identificada o identificable ("persona concernida", como insiste el Convenio).

Se deduce de esta definición, que el concepto de *persona concernida*, a los efectos de determinar de identificación dentro de un procedimiento informatizado de datos, no solamente abarca los rasgos de identificación de la persona de carácter jurídico (como los registros de nacimiento, médico, etc, documento de identificación personal v.gr. Documento Nacional de Identidad DNI en España o Documento de Identidad Nacional DIN o Cédula de ciudadanía en Colombia, Pasaportes, etc), sino también de carácter físico interno v.gr. exámenes de sanguíneos, de líquidos humanos diferentes a la sangre (semen, orina, etc.), exámenes morfológicos (color de piel, facial, dentales, ópticos, de estatura, etc); o de carácter físico externo, con fotografías y huellas humanas y/o tecnológicas (códigos, password o firmas digitalizadas). Estas huellas, se consideran como rasgos diferenciadores de una persona humana de carácter morfológico o tecnológico con incidencia jurídica.

Esta identificación del ser humano o de la "persona concernida" es la que a la luz del Convenio constituye el núcleo central del concepto de datos de carácter personal, muy a pesar de que se sostiene en la E.M., del Convenio, que "persona identificable", es aquella "persona que puede fácilmente ser identificada", sin necesidad de "identificación de personas por métodos complejos" [165]. Quizá en aquella época en que surgió la norma europea, tal proposición pudiera ser válida parcialmente, pero hoy no, pues dicha identificabilidad de las personas, antes y ahora debe incluir métodos y procedimientos científico-técnicos idóneos, máxime si se refiere al tratamiento informatizado de datos personales --con o sin el consentimiento del titular--, que relacionan datos personales contenidos en documentos jurídicos, registros de estado civil, médicos, judiciales, económicos o financieros, etc, en todos los cuales para una debida identificación de la persona se debe emplear medios idóneos de tipo técnico-científicos irrefutables previos al asiento o registro informático o concomitante con éste.

Hoy, el ser humano tiene un derecho a *la identificación* sico-física, como persona humana dotada de cuerpo, mente e inteligencia, válido o validable en todo ámbito social, cultural, político, económico, y sobre todo jurídico o iusinformático. Por lo tanto, no se puede desdeñar ningún método científico-técnico para la plena identificación en todo procedimiento que tenga incidencia en el pleno ejercicio de los derechos y libertades fundamentales de una persona. El Convenio recoge este parecer cuando sostiene que su objetivo prioritario es "reforzar la protección de datos, es decir, la protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal que les conciernen" (M.E.núm. 1).

El concepto de persona concernida también se extiende al de persona "*interesada*", que el Convenio utiliza en varios artículos. Así, *interesado*, "expresa *la idea* según la cual toda persona tiene un derecho subjetivo sobre la información relativa a sí misma, aún cuando tal información haya sido reunida por otras personas

---

(165) Memoria Explicativa del Convenio 108 de 1981. M.E.núm.28. Compilados por HEREDERO HIGUERAS, Manuel. *LEGISLACION INFORMATICA.* Ed. Tecnos, Madrid, 1994, pág.570

(cfr. la expresión inglesa *data subjetc*) [166]

El "*fichero automatizado*" o bancos de datos. Significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado. Aunque en la

E.M., del Convenio eufemísticamente se dice que se prefiere el nombre de fichero al de Banco de datos, porque esta expresión se utiliza "hoy en un sentido más especializado: el de un fondo común de datos accesibles a varios usuarios"[167]. Sin embargo, la diferencia hoy por hoy es simplemente terminológica y de origen idiomático (Banco de datos término anglosajón "*database*" o, Fichero informatizado del término francés "*Fichiers*").

Los Estados Miembros del Consejo de Europa eran conscientes de que día a día crecían por la irrupción de la tecnología TIC y la informática, maneras y formatos de recolectar y almacenar información de todo tipo (incluida las denominadas "personales") con medios informáticos, electrónicos o telemáticos, y que se materializaban en los llamados ficheros o bancos de datos, por regla general. Eran también, conscientes de que los diversos Estados tenían en sus sistemas jurídicos regulaciones sobre el derecho a la intimidad de las personas, la responsabilidad civil, el secreto o la confidencialidad de ciertas informaciones sensibles, etc. Sin embargo, se echaban de menos unas reglas generales sobre el registro y la utilización de informaciones personales y en "especial, sobre el problema de como facilitar a los individuos el ejercicio de un control sobre informaciones que, afectándoles a ellos, son colectadas y utilizadas por otros" (M.E.núm.3). En tal virtud, se decidió concretar además de el concepto de datos de carácter personal, qué debe entenderse por fichero o banco de datos para proteger los derechos y libertades fundamentales de la persona y facilitar el autocontrol de los mismos por parte de la persona concernida.

El concepto de fichero o banco de datos informatizados, comprende "no solamente ficheros consistentes en conjuntos compactos de datos, sino a si mismo conjuntos de datos dispersos geográficamente y reunidos mediante un sistema automatizado para su tratamiento" (M.E.núm. 30 *ab initio*).

La definición de fichero "automatizado" para diferenciarlo del fichero o banco de datos mecánico o manual, resulta reiterativo cuando menos desde el punto de vista terminoló

---

(166) Ibídem., pág. 570.

(167) El M.E.núm. 30 ab initio, sostiene que la "expresión ´fichero automatizado´ ha sustituido a la de ´banco de datos electrónico´ utilizada anteriormente en Resoluciones (73)22 y (74)29 y en algunas leyes nacionales. Por ello, en el transcurso de la investigación utilizaremos indistintamente fichero o banco de datos para referirnos al mismo concepto.

gico, cuando al final sostiene que ese conjunto de informaciones deben estar sometidas a un tratamiento igualmente "automatizado" (que mejor sería decir informatizado [168]). Sin embargo, esta observación es de menor entidad, frente a la significancia de la inclusión de un término imprescindible en el tratamiento lógico de entrada (E/) y salida (/S) de información por medios informáticos, como lo es el de fiche- ro o banco de datos informatizados. Esta aclaración delimita a su vez, el ámbito de aplicación del Convenio, al tratamiento informatizado de los datos o información de carácter personal, a diferencia de la Recomendación de la OCDE de 1980, que abarcaba incluso el tratamiento no informatizado de datos personales, aunque la definición siguiente desmienta tal diferenciación, al menos en toda su integridad.

En efecto, por *"tratamiento automatizado",* se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión (art. 2, c). Este tratamiento de datos se extiende a los datos de carácter personal en los sectores público y privado (art. 3-1, del Convenio) [169] .

Las acciones de tratamiento lógico de la información, que se traducen en fases o ciclos informatizados, según la definición de tratamiento automatizado del Convenio puede efectuarse total o parcialmente con procedimientos informáticos, con lo cual se introducen métodos de tratamiento mixtos de la información, en los cuales participan acciones mecánicas o manuales e informáticas.

---

(168) Preferimos decir "informatizado", porque entre otras razones que se dan a lo largo de la investigación, existen estrechos vínculos entre la información obtenida (cualquiera sea esta, y más si es de tipo personal) con "la informática documental", según los términos del profesor *LOPEZ MUÑIZ-GOÑI,M* (En: Informática Jurídica Documental) que utiliza métodos y procedimientos informatizados en el tratamiento lógico, sistemático y analítico de la información que ésta proporciona y no solamente un tratamiento robótico o "automático" de la información, tal como lo hacen los cajeros electrónicos, sistemas electrónicos de detección de personas o cosas, etc. Es un tratamiento logicial con medios informáticos, electrónicos o telemáticos y no simplemente cibernético o robótico aunque éste sea la base del mismo.

(169) El Convenio se aplica al sector público y privado. "Si bien es cierto que la mayor parte de la circulación internacional de datos tiene lugar dentro del marco del sector privado, el convenio reviste, no obstante, gran importancia para el sector público y ello por dos razones: en primer lugar, el art. 3 impone a los Estados miembros la obligación de aplicar los principios de la protección de datos aun en el caso del tratamiento de ficheros públicos --que es el supuesto normal-- totalmente dentro de sus fronteras nacionales. En segundo lugar, el convenio ofrece asistencia a los interesados que deseen ejercer su derecho a ser informados del registro que de ellas lleve una autoridad pública en un país extranjero. La distinción sector público- sector privado no aparece en

las demás disposiciones del convenio, sobre todo porque esta nociones pueden tener significados distintos de un país a otro...” (M.E.núm. 33)

El concepto técnico-jurídico abierto de *tratamiento de datos personales*, abre la posibilidad a la interpretación de que el Convenio no sólo regule el tratamiento informatizado de la información, sino también el no informatizado siempre y cuando contenga alguna parte, acción o fase de carácter informática. Esto es posible cuando la fase inicial o de recolección de información en un tratamiento lógico o informatizado es carácter mecánico o manual [170].

Las fases o ciclos del tratamiento informatizado, según el Convenio se inician con el *registro de datos* y frente a él todas las acciones (u “operaciones aritméticas”, guar- dando con ello más relación al tratamiento robótico de la información que al lógico o sistémico) subsiguientes que pueden realizarse: modificación, borrado, extracción o difusión de la información [171]. Todas estas acciones a excepción de la última, son componentes de una acción eminentemente tecnológica realizable con los datos (o “files”: archivos o registros), más que jurídica; puesto que, sí se quería referir a las acciones técnico-jurídico realizables con cualquier tipo de datos, debió hacerse mención a las fases de recolección, almacenamiento, registro, conservación, rectificación, bloqueo y cancelación de la información, tal como lo hiciera la LFAPD de 1977 [172], y posteriormente, la Recomendación de la OCDE de 1980.

Sin embargo, el contexto del Convenio aclara la deficiente definición de *tratamiento automatizado*, cuando se refiere: a) a los principios y derechos que tiene toda persona cuando han sido sometidos a tratamiento informatizado los datos personales que le conciernen y, b) al hacer mención expresa a la fase de recolección (en los artículos 5-a y 12 del Convenio [173]) y de transmisión “internacional” (o fase de comunicación) de datos, como fases ineludibles y/o posibles del tratamiento informatizado o no de datos. Esto a pesar de la insistencia de la E.M., núm. 31 *ab initio* del Convenio al excluir la fase de recolección o colecta de información “de la noción de

---

(170) Véase, parte III, *in fine*, sobre el procedimiento informatizado de datos personales en su fase in del tratamiento.

(171) La voz “difusión”, según la E.M.núm. 31 ab initio,” es un término genérico que abarca tanto la revelación de información a una persona (o a varias personas), como la consulta de la información por tales personas”

(172) Veáse, aparte 4.2.1. y ss, Parte I.

(173) El Convenio utiliza los términos “obtener” o “reunir”, para hacer mención a la fase inicial de recolección o colecta de datos. En efecto, el art. 5, a), expresa: “Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) *Se obtendrán* y tratarán leal y legítimamente”, y el Art.12., al referirse a los “Flujos transfronterizos de datos de carácter personal y el derecho interno : 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado *o reunidos* con el fin de someterlos a ese tratamiento”.

tratamiento” de datos, con unos argumentos poco convincentes [174].

La *Autoridad "controladora del fichero",*se considera a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero informatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les deberá aplicar.

La definición contiene un concepto ampliado del *ente almacenante* que trae la LFAPD, en el art. 1-1., y a la vez, una conceptualización casi idéntica a la de “responsable del fichero” contenida en la Recomendación de la OCDE de 1980, art.1-a. En efecto, la entidad almacenante atribuible a cualquier persona, entidad, servicio o institución pública o privada, tiene como función primordial el almacenamiento (que incluye según la ley alemana, las fases de recolección, registro y conservación) de datos por sí mismo o por encargo a otro. En cambio, “el responsable del fichero”, tanto en el la Resolución de la OCDE, como en el Convenio 108 de 1981, abarca otros ciclos o fases como funciones del tratamiento informatizado de los datos o informaciones personales, tales como la transmisión de datos, la determinación de la finalidad del fichero, la categorización de los datos, el registro y hasta “cuáles operaciones se les aplicarán” (art. 2, d), del Convenio), respectivamente.

El *Responsable del fichero* se diferencia en uno y otro cuerpo normativo (OCDE y Convenio) en la circunstacia de que el “responsable del fichero”, en el Convenio es única y “exclusivamente la persona o ente que en última instancia responde de la gestión del fichero, pero no aquellas otras personas que llevan a cabo las operaciones del tratamiento de conformidad con las instrucciones del responsable del fichero” (M.E.núm.32).

Este concepto de *Responsable del fichero*, cuando menos, determina dos aspectos importantes en el tratamiento informatizado de datos: por un lado, la

exclusión de cualquier grado o nivel de responsabilidad de los que realizaran actividades de tratamiento por encargo; y de otra, que la determinación del responsa-

---

(174) Se dice que "ante el rápido desarrollo de la tecnología del tratamiento de la información, se consideró conveniente enunciar una definición bastante general de "tratamiento automatizado", susceptible de una interpretación flexible".Y según, la autointerpretación del legislador comunitario del Convenio, la colecta queda excluida del concepto "tratamiento".

ble del fichero, lleva aparejada una garantía para las personas concernidas con el tratamiento de datos personales, la cual es, que puedan en todo momento identificar plenamente al responsable del fichero [175].

4.3.2.2. PRINCIPIOS Y EXCEPCIONES FUNDAMENTALES EN EL TRATAMIENTO Y CIRCULACIÓN DE DATOS .

El Convenio 108 del Consejo de Europa de 1981, sobre protección de las personas en relación con el tratamiento informatizado de datos personales, no sólo "refuerza" la protección jurídica de los individuos en relación al tratamiento informatizado de información de carácter personal, tal como se prevé en el preámbulo, la E.M., núm. 1, y en el propio texto (art. 1); sino que además propone una armonización normativa en el ámbito competencial del Consejo de Europa. Quizá uno de los aspectos capitales en los cuales el Convenio más apuesta por la armonización normativa a nivel europeo, es precisamente en la estructuración de los principios y excepciones fundamentales, así como en los derechos subsecuentes para los titulares de datos personales que de aquellos se derivan. En efecto, el Convenio persigue homogeneizar todo lo atinente a la regulación de la protección de los titulares de los datos prevista en las leyes protección de aquellos dictados hasta ese entonces (v.gr.Alemania, Suecia, Suiza, Francia, Noruega, Luxemburgo, Portugal, etc), como también aquellas otras leyes que se dictaron a su amparo y guía, como es el caso de la Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal española (L.O. 5/1992, de 29 de Oct.).

En efecto, las Comisiones y subcomisiones encargadas del estudio, análisis y proposición del texto definitivo del que luego fuera el Convenio Europeo de 1981, reestructuró los principios inmersos en las leyes europeas de protección de datos y en forma mancomunada abordó la tarea de su proposición final con el grupo de

expertos del Comité respectivo de la OCDE [176] . Especial atención le dedicó a los principios de

---

(175) En efecto, el art. 8., del Convenio 108 de 1981, al hacer referencia a las denominadas "Garantías complementarias para la persona concernida", sostiene que cualquier persona deberá poder: "a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como *la identidad* y la residencia habitual o el establecimiento principal de *la autoridad controladora del fichero.*
(176) M.E.núm. 14, "Cooperación con la OCDE y con la CEE".

la libre circulación y seguridad de los datos [177] . Quizá por ello, los principios como excepciones al tratamiento informatizado de datos personales en uno y otro cuerpo normativo comunitarios resultan coincidentes, con la diferencia de que en el Convenio de Estrasburgo, estos y aquellas tienen una especial regulación que los convierte en la columna vertebral del tratamiento informatizado de datos personales.

En efecto, el Convenio Europeo como regla general establece que los principios y excepciones al tratamiento informático de datos, rigen en todo el tratamiento o procedimiento informatizado de datos personales y no en forma exclusiva y/o excluyente de una fase o etapa de dicho tratamiento (v.gr. recolección, almacenamiento, registro, conservación, etc.). Así se deduce de la redacción dada a los arts. 5 a 9 del Convenio. El sistema de principios y excepciones están ligados entre sí, pues unos y otros tienden a garantizar y proteger los derechos, libertades públicas, intereses legítimos "y los valores fundamentales en una sociedad democrática" (M.E.núm. 55).

Es aquí donde halla eco y sentido el denominado "*núcleo irreductible*"[178] , basado en la catalogación de los principios y excepciones fundamentales del tratamiento informatizado de datos personales, con capitales fines y objetivos de protección y garantía de derechos y libertades fundamentales (no sólo el derecho a la intimidad, como se ha generalizado), el debido y oportuno cumplimiento que los Estados deben observar en la implementación en el ordenamiento jurídico interno (es decir, armonización legislativa) y la reducción al mínimo de los posibles conflictos de las leyes o de jurisdicción.

4.3.2.2.1. PRINCIPIOS FUNDAMENTALES EN EL TRATAMIENTO Y TRANSMISION DE DATOS PERSONALES.

---

(177) M.E. núm. 16. "La comisión de las Comunidades Europeas, que ha llevado a cabo estudios sobre la armonización de las legislaciones nacionales dentro del marco de la Comunidad con relación a los flujos internacionales de datos y las posibles distorsiones de la concurrencia, así como sobre los problemas vinculados a la seguridad de los datos, mantuvo estrecho contacto con el Consejo de Europa."

(178) Institución de derecho público que se explica en relación con los principios y *per se*. En efecto, "los principios del ´núcleo irreductible´ reconocen a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento automatizado de datos de carácter personal" (M.E.núm. 20 *in fine*).

Ahora bien, hagamos referencia a los principios en relación con las fases del tratamiento informatizado de datos que es donde tienen aplicabilidad y vigencia.

4.3.2.2.1.1. FASE DE RECOLECCION DE DATOS.

En la *fase inicial o de recolección de los datos personales,* son aplicables los principios siguientes: a) De lealtad y legitimidad (art.5-a,); b) De Prohibición excepcionada a la recolección de datos pertenecientes al "núcleo duro de la privacy" anglosajona [**179**] (art. 6); y, c) De información en la recolección, sobre los objetivos y fines de la misma (art. 8).

Estos principios se hallan en el Convenio bajo los epígrafes de "calidad de los datos", "categorías particulares de los datos" y "garantías complementarias para la persona concernida".

El principio de lealtad y legitimidad, como principio de causa y efecto entre el objeto del tratamiento (datos) y su actividad (recolección), se entiende que los datos que se van a obtener, recoger o recolectar debe pertenecer a una persona identificada o identificable, procesarse con métodos informáticos idóneos que permitan no vulnerar los derechos y libertades fundamentales del titular de los mismos y se proceda de conformidad con el ordenamiento jurídico vigente en cada Estado y en concordancia con las normas comunitarias. Queda proscrita toda recolección de datos en forma ilícita, ilegítima, indebida, inoportuna o expresamente prohibida. Quizá por esto último resulta incompleta la calificación de este principio como "principio de legalidad" de los datos, que algún sector de la doctrina ibérica lo nomina (*Castells, Souviron, López*, etc), pues la ley queda transvasada, cuando se

involucra el interés estatales o personal, el criterio de la oportunidad del tratamiento, etc.

En principio, está prohibida la recolección de datos de carácter personal denominados "sensibles" [180] que revelen el origen racial, las opiniones políticas, las

---

(179) Comentado por el profesor MORALES PRATS, Fermín. *COMENTARIOS A LA PARTE ESPECIAL DEL DERECHO PENAL*. En: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Ed. Aranzadi, Pamplona, 1996, pág. 310 y ss.

(180) Según *E. Vilariño*, datos sensibles son "aquellos datos personales que se refieren a las características morales o físicas que, en principio, no son de interés para los demás y no afectan en general a la sociedad y cuyo conocimiento, en cambio, puede perjudicar injustificadamente los derechos e intereses legítimos de esas personas", p. 54. Citado por SOUVIRON, José M. *EN TORNO A LA JURIDIFICACION DEL PODER INFORMATICVO DEL ESTADO.* R.V.A.P.Núm. 40, Sep-Dic., Bilbao, 1994, cita núm. 67 pág.153.

convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales (art. 6) [181].

4.3.2.2.1.2. FASE DE ALMACENAMIENTO DE DATOS.

En *la fase de almacenamiento* de datos, serán aplicables los principios de: a) Exactitud del contenido (o "veracidad", según *Souvirón* [182]) y de sujeción a la revisión y actualización (art. 5-d); b) De prohibición excepcionada de los datos denominados "sensibles" (art.6); y c) De información en el almacenamiento de datos sobre los objetivos y fines del mismo (art. 8).

4.3.2.2.1.3. FASE DE REGISTRO DE DATOS.

En la *fase de registro de los datos personales*, que es la etapa sobre la cual más incide el Convenio Europeo, quizá por las implicaciones de tipo socio-jurídico que se derivan de dicha actividad informatizada de datos, pues ésta sobreviene con carácter definitivo en tanto no haya causas para suspenderla, suprimir o cancelarla de conformidad con el ordenamiento jurídico vigente. Pareciera , por la redacción inicial del Convenio que la protección de los titulares de los datos se inicia con el registro de los mismos y no antes. Sin embargo, una recta interpretación del Convenio extiende la protección al momento mismo de la recolección de datos, haciendo énfasis en la etapa del registro porque supuestamente más afloran los

síntomas de vulnerabilidad, aspecto éste que es más apariencia que realidad, como se ha visto.

Los principios aplicables a esta etapa del tratamiento informatizado son: a) De compatibilidad de las finalidades (art. 5-b); b) De adecuación, pertinencia y no excesibilidad de las finalidades (art. 5-c); c) Prohibición excepcionada del registro de datos personales denominados "sensibles" (art.6); d) Principio de información en el registro de datos (art. 8); y . e) Principio de "Seguridad de los datos" (art. 7).

Se destacan en esta etapa los principios de información y seguridad de los datos, por cuanto, en puridad jurídica es aquí donde nace el derecho de *habeas*

---

(181) Sobre el particular ahondaremos en su tratamiento en la Parte III y IV., de esta investigación. Por ello, remitimos a lo allí sostenido.

(182) SOUVIRON, José M. Ob. cit. ut supra. pág. 152.

data[183] y los subsecuentes derechos que este conlleva. Efectivamente, tras el ejercicio el derecho de la información y conocimiento por parte del titular de los datos, de terceros, de personas autorizadas o no, las personas naturales, jurídicas, públicas o privadas encargadas del tratamiento (o responsables) de datos toman las necesarias medidas de seguridad para la protección de datos de registrados en ficheros informatizados, a fin de evitar la destrucción accidental o no autorizada, la pérdida accidental o el acceso, la modificación o la difusión no autorizados.

En tal virtud, aquí se ponen en juego las que el Convenio en el artículo 8, llama "Garantías complementarias para la persona concernida", dentro de las cuales cualquier persona podrá: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos de "calidad de los datos" y "categoría particular de datos"; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, luego de conocer la existencia de un fichero con los datos

del concernido o de obtener a “intervalos razonales” la confirmación de tal existencia o no.

4.3.2.2.1.4. FASE DE CONSERVACION DE DATOS.

En la *fase de conservación de los datos,* se aplicará los siguientes principios: a) De identificación del concernido y de compatibilidad de las finalidades. En ejercicio de este principio, se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado (art. 5-e,); b) De Prohibición excepcionada en la conservación de datos personales considerados “sensibles” (art.6);

---

(183) Se considera un derecho fundamental, que según *Fairen Guillen*,” ya no (solo) es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data* Tales son las ideas generalmente admitidas hoy entre juristas y en el Derecho comparado, que ofrece una de las vías para determinar el contenido esencial de un derecho fundamental (S.T.C. 11/1981)” en el derecho español. Cfr. FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL SUGERIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992*. En: Revista de Derecho Procesal. Núm.3, Madrid, 1996, pág.530.

c) De Seguridad de los datos (art. 8); y d) De información en la conservación de datos.

4.3.2.2.1.5. FASE DE TRANSMISION DE DATOS. EN PARTICULAR, EL “FLUJO INTERNACIONAL DE DATOS” [184] .

En la *fase de transmisión, flujo o movimiento de los datos,* a la que el Convenio también le ha prestado especial cuidado y tratamiento, rigen los principios previstos bajo los epígrafes de “calidad de datos”, “categoría particular de datos”, “Seguridad de datos” y “garantías complementarias para la persona concernida”, que antes hemos referenciado, pues al fin y al cabo la transmisión de datos es otra fase más del tratamiento de datos, tal como lo sostiene el art. 12.1 del Convenio Europeo [185]. Pero además, se aplicará un principio fundamental y específico para esta fase del tratamiento informatizado de datos personales, cual es la “*libre circulación de datos*”[186], que desde la Recomendación de la OCDE de 1980, ya había sido planteado y sustentado.

Esta fase del tratamiento informatizado de datos personales es tan importante como delicada, pues los Estados que poseían medidas legislativas protectoras de dicho tratamiento habían preparado y aplicado sus normas hacia el interior de sus zonas geográficas, pero no estaban preparados inicialmente para afrontar los dificultades sobrevenidas por la transferencia de datos entre Estados. La creación de "bancos de datos internacionales", con diferentes fines, objetivos y actividades eviden-

---

(184) La M.E.del Convenio Europeo "especifica el alcance de la noción de *flujos internacionales*, ha sido redactado de tal manera que tenga en cuenta la gran diversidad de los factores determinantes del modo en que los datos son transferidos: modalidad de representación (texto libre o codificado), soporte (papel, tarjeta perforada, cinta perforada, cinta magnética, disco, etc), medio de transporte (transporte físico, correo, enlace de telecomunicación conmutada por circuito o paquetes), interfaz (ordenador con terminal, ordenador con ordenador, manual con ordenador, etc), el circuito dedicado (directo desde el país de origen al país de destino, o a través de uno o varios países de tránsito), las relaciones entre el emisor y el destinatario (pertenecientes ambos a una misma organización o a distintas organizaciones), etc. (M.E.núm. 63). El tema será vuelto a tratar en la parte III y IV de esta investigación.

(185) Artículo 12. Flujos transfronterizos de datos de carácter personal y el derecho interno 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal *que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento"* (Cursivas nuestras).

(186) Este principio fundamental en el tratamiento y transmisión de datos personales, tanto para los individuos como para los Estados, se erigió, "habida cuenta de la rápida evolución de las técnicas de tratamiento de la información y del desarrollo de la circulación internacional de datos...(y de que era) conveniente crear unos mecanismos a escala internacional que permitan a los Estados tenerse informados mutuamente y consultarse entre sí en materia de protección de datos" (E.M. núm. 11 *in fine*).

ció más aún dichas dificultades, pero a la vez, con la generalización de las transferencias internacionales en los ámbitos sociales, políticos, culturales, jurídicos y sobre todo económicos de la UE, se puntualizó y potenció toda clase de medidas de seguridad, eficacia, oportunidad y celeridad de la transmisión/emisión de datos personales, para eliminar las dificultades y aumentar el flujo necesario de información entre Estados, sin mayores riesgos que los sobrevenidos de actividades indebidas, ilegales o no autorizados, tanto de tipo técnico como jurídico. En efecto, así ocurrió con las variopintas transacciones comerciales (v.gr. agencias de viajes, operaciones bancarias, cajeros automáticos: tarjetas de crédito, debido, etc.), las transferencias en actividades personales privadas o públicas (.v.gr. Bancos de datos médicos, investigativos, bibliotecológicos, estadísticos, etc); o en fin, para transmitir información de un lugar geográfico transfronterizo a otro sin las debidos controles (técnicos o jurídicos, según la M.E.núm. 8), con fundamento en los adelantos de las telecomunicaciones, la informática, o la unión de las dos: la comunicación electrónica o telemática.

En especial, --se decía en el E.M.núm.9-- existe el temor de que los usuarios se sientan tentados a "hurtarse" a los controles impuestos por la protección de datos desplazando sus operaciones, en todo o en parte hacia "paraísos de datos", es decir, a países que tengan leyes de protección de datos menos rigurosas o que carezcan de leyes de protección de datos. Aunque algunos otros Estados para evitar estos riesgos han previsto en su Derecho interno controles jurídicos especiales, como las "autorizaciones de exportación de datos", las cuales pueden resultar excesivos o insuficientes, frente a la avalancha de crecimiento de las transmisiones electrónicas de datos entre Estados.

El Convenio, en consecuencia, establece que un Estado no podrá "prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio" de otro Estado, so pretexto "de proteger la vida privada", salvo: a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación del otro Estado (*o Parte*) establezca una protección equivalente; b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otro Estado, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación del Estado a que se refiere el comienzo del presente párrafo (art. 12 *in fine*)..

En estas transmisiones interestatales, el mayor flujo de circulación de datos lo ocupan las transferencias de datos de carácter personal, por ello, el Convenio plantea como regla general, la *libre circulación de información* , como principio fundamental, tanto para los individuos como para los Estados (o "pueblos", según la E.M.núm.9) y como excepciones, las directrices previstas con carácter de *numerus clausus* para algunas categorías de datos personales (básicamente los denominados *sensibles*) o ficheros que los contengan y para aquellas transmisiones triangulares entre Estados y uno de los cuales no pertenezca al Consejo europeo.

Si no fuese así, "tales controles (como el de la autorización, p.e.) podrían crear trabas a la libre circulación de la información", erigida como principio fundamental en el tratamiento y transmisión de datos personales entre Estados.

"Había que encontrar, por tanto, una fórmula que garantizara que la protección de datos a escala internacional no vulneraría este principio" (M.E. núm. 9 *in fine*). Se trata en últimas de conciliar [187] dos aspectos capitales en el tratamiento y transmisión de datos personales, que tienen la particularidad de ser concurrentes y aparentemente excluyentes: por un lado, la protección de datos; y por otro, la libre circulación de los mismos. Concurrencia que se consigue cuando toda transmisión o flujo de datos debe preveer cierto mínimo de garantías o de protecciones, pero no de controles especiales ni menos rigurosos que pudieran excluir la libre circulación de los datos. De ahí el establecimiento de una regla general con sus taxativas excepciones.

La E.M., del Convenio sustenta una serie de características especiales referentes a los flujos internacionales de datos, las cuales en su conjunto reafirman la regla y excepciones anotadas.

En efecto, se establece que con base en el principio del *núcleo irreductible* que reconoce a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento informatizado de

---

(187) Ese es el objeto principal del art. 12 del Convenio de Europa, "conciliar las exigencias de protección eficaz de los datos con el principio de la libre circulación de la información independientemente de la existencia de fronteras, consagrado por el artículo 10 del Convenio Europeo de los Derechos del Hombre" (E.M. núm. 62).

datos, y como tal, al obligarse a aplicarlos los Estados y miembros, "tienden a suprimir entre ellos las restricciones de los flujos internacionales de datos, evitando que el principio de libre circulación de datos sea puesto en tela de juicio por alguna forma de proteccionismo" (M.E.núm. 20 *in fine*).

Respecto de la transmisión o flujos de datos personales calificados de sensibles (relativos al origen racial, origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, la salud [188] o a la vida sexual, según el art. 6 del Convenio) se establece, al menos dos directrices para que un Estado justifique la derogación de las garantías que el Convenio ofrece a esta clase especial de datos personales. Estas son:

a) Cuando las medidas específicas de protección de tales datos fueren sensiblemente distintas de las disposiciones del derecho de los demás Estados que hicieren referencia a tales datos y, en especial, cuando tales medidas ofrecieren, de conformidad con el art. 1, (es decir, que ninguna de las disposiciones del capítulo II, se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Estado, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio) un nivel de protección que transcendiere las normas mínimas contenidas en el Convenio.

b) Cuando determinados datos o ficheros que no estuvieren previstos dentro de los denominados datos sensibles, estuviesen sujetos a garantías especiales.

No será lícita la derogación, en estos casos, si el Estado destinatario ofreciere una protección equivalente. v.gr. Si un Estado somete los flujos internacionales de datos a una autorización especial, no puede negarse otro Estado, so pretexto de razones de protección de la intimidad, a conceder una tal autorización si el país receptor concede una protección equivalente (E.M. núm. 69 *in fine*).

Respecto de la *transferencias triangulares de datos personales*, o sea, aquellas

---

(188) Los datos de carácter personal relativos a la salud, fue cuidadosamente estudiado por el Comité de expertos de protección de datos dentro del contexto de sus trabajos sobre los bancos de datos médicos. Tal noción abarca las informaciones concernientes a la salud pasada, presente y futura, física y mental, de un individuo. Puede tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas (E.M. núm. 45).

que tienen lugar en dirección a un Estado no contratante a través de un Estado contratante, la derogación sólo puede ser invocada si está previsto que los datos transferidos se encuentren en un Estado contratante sólo en tránsito. No deberá ser invocada sobre la base de la mera presunción o expectativa de que los datos transferidos a otro Estado contratante pudieran, en su caso, ser transferidos a un Estado no contratante (E.M. núm. 70).

4.3.2.2.2. EXCEPCIONES AL TRATAMIENTO INFORMATIZADO DE DATOS Y A LOS PRINCIPIOS. LAS “RESTRICCIONES”.

Para establecer un régimen jurídico de excepciones en un ámbito interestatal, se debe tener en cuenta, al menos dos reglas primordiales: el objeto y fin de la norma jurídica y la taxatividad en la enunciación de los supuestos de excepciones. Todo ello, para que los Estados no “tropiecen con dificultades en cuanto a la interpretación de la excepción, pues ello podría obstaculizar gravemente la aplicación del Convenio” (E.M.núm. 35 *in fine*).

Por lo primero, el Convenio Europeo, según el art. 1., establece que su objeto y fin es garantizar, en los territorios de los Estados miembros, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus *derechos y libertades fundamentales*, concretamente su derecho a la intimidad (o “vida privada”), con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").

Respecto de lo segundo, es decir, la regulación *numerus clausus* de los supuestos de excepciones, están previstas en el art. 9 del Convenio, con las siguientes anotaciones:

La regla general, para las excepciones al tratamiento informatizado de datos, consiste en la no admisión de excepción alguna contra los principios fundamentales previstos para las fases o etapas del tratamiento informatizado de recolección, almacenamiento, registro y conservación de datos personales, salvo que estuviere: prevista en el ordenamiento jurídico vigente del Estado miembro y constituya una medida necesaria en una *sociedad democrática*, para: a) la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; y, b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

Estas excepciones a la excepción de los principios fundamentales del tratamiento informatizado, están inspiradas en el Convenio Europeo de los Derechos del Hombre (arts. 6, 8, 10 y 11). Así mismo, la expresión “medida necesaria” en una sociedad democrática, constituye una noción fruto de los acuerdos de la Comisión y el Tribunal de los Derechos Humanos, por la cual, resulta claramente que los criterios de tal concepto no pueden ser fijados para todos los Estados y en todo

momento, sino que deberían ser considerados a la luz de la situación dada en cada Estado [189].

Las excepciones a la regla general tienen como fuente dos grandes ramales, a saber: los intereses fundamentales de los Estados y los intereses particulares de la persona humana.

En efecto, la enumeración taxativa dentro de las causales exceptivas al tratamiento y principios fundamentales de los datos obedece básica y exclusivamente a la delimitación conceptual de los que se consideran intereses principales de los Estados, es decir, de aquellas instituciones socio-jurídicas ; tales como, la seguridad del Estado [190], seguridad pública , intereses monetarios del Estado [191] e infracciones penales [192]; y por su puesto, a fin de evitar que en la aplicación del Convenio los Estados puedan tener un "margen de maniobra demasiado amplio" en la interpretación y aplicación de las mismas y conserven la facultad de "rehusar"[193] la

---

(189) Las excepciones se limitan a las que son necesarias para proteger los "valores fundamentales en una sociedad democrática". (E.M.núm. 55).

(190) Se entiende por *Seguridad Pública*, en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado (E.M.núm. *56 in fine*).

(191) *Intereses monetarios del Estado*, comprende todo aquello que contribuye a facilitar al Estado los recursos financieros de su política. v.gr. La recaudación de los impuestos y al control de cambios. (E. M. núm. 57 *ab initio*).

(192) *Represión de los delitos*, comprende tanto la investigación de los delitos como su persecución (E.M. núm. 57 *in fine*).

(193) *Artículo 16. Denegación de peticiones de asistencia*. Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 ("Cooperación entre Estados) o 14 (Asistencia a las personas concernidas que tengan su residencia en el extranjero) del presente Convenio, solamente podrá negarse a atenderla si: a) La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder; b) la petición no está conforme con lo dispuesto en el presente Convenio; c) atender a la petición fuese incompatible con la soberanía, la seguridad o el orden público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

aplicación del Convenio en casos concretos por motivos de importancia ponderada (E.M.núm. 56).

En cuanto a la enunciación taxativa de las causales de excepción al tratamiento y principios básicos de los datos previstas en el literal b), sobre protección de la persona concernida están fundadas en los intereses particulares de

la persona humana, tales como los del *interesado* (p.e., información psiquiátrica) o de *terceros* (p.e., la libertad de prensa, secretos del comercio, etc).

Conjuntamente con este marco de excepciones, el Convenio presenta las que llama "restricciones" al ejercicio de los ciertos derechos de la persona concernida y presentes en los "ficheros automatizados" de datos personales que se utilicen con fines estadísticos o de investigación científica [**194**], cuando no existan manifiestamente riesgos de atentado a la intimidad ("vida privada") de las personas concernidas (art. 9-3).

Jurídicamente están restricciones no se consideran excepciones, sino limitaciones al ejercicio de algunos derechos impuestas por razones expresamente previstas en el ordenamiento jurídico, y como tal, pueden ser preventivas (*in tempore*) o modales (eliminación del riesgo o vulnerabilidad). Sin embargo, en la *praxis,* estas restricciones pueden esconder verdaderas instituciones nugatorias de derechos, aún cuando fueren preventivas o modales.

Las restricciones al ejercicio de algunos derechos en las circunstancias y para ciertos ficheros o bancos de datos previstos en el Convenio, se extiende a aquéllos derechos de la persona concernida que como "garantía complementaria" ostenta en el transcurso del tratamiento informatizado de datos personales. Esos derechos son los componentes del derecho de *habeas data* que inicia con el de información. En efecto, se admite la restricción al ejercicio de los siguientes derechos: a) *De confirmación* de la existencia o no de un fichero con datos del concernido, así como el de comunicación de dichos datos; b) *De rectificación* o borrado de datos, según fuere el caso, si se des-

---

(194) En los ficheros o banco de datos estadísticos la posibilidad de limitar el ejercicio de los derechos de los interesados, se centra en las "operaciones de proceso de datos que no llevaren aparejado riesgo alguno... en la medida en que se trate de datos presentados en forma agregada y separada de los identificadores. Igual los ficheros de datos científicos de conformidad con una recomendación de la Fundación Europea de la Ciencia (E.M.núm. 59 *in fine*).

conoce los principios fundamentales del tratamiento informatizado de datos (recolección, almacenamiento, registro y conservación) o la consideración de ser datos sensibles; y c) *De recurso,* ante las autoridades competentes, si no se atiende o se desconoce los anteriores derechos.

4.4. ESPAÑA: LEY ORGANICA DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL.

La Ley orgánica de regulación del tratamiento automatizado de datos de carácter personal, L.O. 5/1992, Oct. 29, (en adelante LORTAD) que entró en vigor el 31 de enero de 1993 (novísima ley que clama reformas) [195], no es en estricto rigor jurídico una "Ley Española de informática", como lo sostiene Fairen Guillen [196], a pesar de que se refiera a las etapas, principios, derechos-deberes y recursos del tratamiento informático de datos personales, ni tampoco es una ley orgánica que regula en forma plena el tratamiento informatizado de datos personales de titularidad pública y de titularidad privada, pues además de las excepciones *numerus clausus*[197],

---

(195) La LORTAD LO 5/1992, de 29 de Octubre, entró en vigor práctica como jurídicamente, el 31 de enero de 1993, puesto que la disposición final cuarta, expresamente sostenía que aquella se producirá tres meses después de la publicación en el Boletín Oficial del Estado (BOE 31-10-1992, núm. 262, [pág. 37037]). Terminaba así con la existencia de la disposición transitoria primera de la Ley Orgánica 1/º982, de 5 de mayo, de *protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* y por la cual, se aplicaba la mencionada ley, aunque en un ámbito de comprensión legislativa y aplicabilidad hermenéutica restringidos (pues se refiere sólo "a las intromisiones ilegítimas derivadas del uso de la informática) a todos aquellos aspectos referentes al tratamiento informatizado de datos personales, la protección de los derechos y libertades fundamentales e intereses legítimos y el uso de la informática, según lo estipuló la disposición única derogatoria de la LORTAD. La vida y derogación jurídicas de unas normas jurídicas que regulan el tratamiento informatizado de datos personales en España, estaba marcada no sólo temporal sino espacialmente de una etapa fructífera de cariz legislativo comunitario y estatal europeos en materia de protección de los titulares de los datos personales, más que de los datos *per se*, cuando son sometidos a procesos informáticos con soportes y medios informáticos, electrónicos o telemáticos, como hemos. Quizá esta sea una de las fundamentales razones para proponer reformas legislativas a la actual LORTAD y sus correspondientes Reales Decretos que la reglamentan. Razones que al interior de España se han ampliado y plasmado en los variopintos recursos de inconstitucionalidad de la LORTAD, ante la Tribunal Constitucional Español, como veremos más adelante.

(196) FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL SUGERIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992*... Ob. ut supra cit., pág. 523 y ss.

(197) El régimen de protección de los datos de carácter personal que se establece en la presente LORTAD, no será de aplicación: a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general. b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales. c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o

que deja por fuera de su regulación ciertos tipos, categorías y clasificaciones de procedimientos informatizados, hace mayor incapie en el tratamiento informatizado de datos de carácter particular.

La LORTAD es una ley que persigue inicialmente la protección de la trilogía de derechos previstos en el art. 18.4 CE: el honor, la intimidad y la propia imagen "y el pleno ejercicio de sus derechos". Luego, en el contexto de la ley se hace se hace énfasis en la protección del derecho a la intimidad, por considerarlo el más vulnerable dentro del tratamiento informatizado de datos, pese a que en la praxis de nuestra *sociedad informatizada,* los nuevos fenómenos tecnológicos TIC y la informática, tienen como características su alta porosidad y penetrabilidad en todos los sectores de la vida humana. Sin embargo este énfasis de la LORTAD, es explicable pues por herencia temática, las anteriores leyes protectoras de datos desde las estatales de las década de los 70´s y 80´s, así como las normas internacionales (La Resolución de la OCDE de 1980) y las comunitarias europeas (Convenio 108/1981), concibieron sus leyes garantistas teniendo como núcleo el derecho a la intimidad, llamándolo indistintamente "privacy", "vida privada", "privacidad", etc. Más aún, las nuevas leyes comunitarias europeas protectoras de los titulares de datos personales, como veremos, en forma expresa dirigen el ámbito garantísta en forma casi exclusiva y excluyente hacia el derecho de la intimidad (Directiva 95/46/CE, Directiva 97/66/CE).

En el ámbito de la LORTAD, la protección enfatizada del derecho a la intimidad (o de la "privacidad", según *Heredero Higueras y González Navarro,* aún cuando sólo en la E.M. núm. 1 y no en el texto de la norma jurídica se hace la distinción entre la

---

----Continuación nota 197---
repertorios oficiales. d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos. 3. Se regirán por sus disposiciones específicas: a) Los ficheros regulados por la legislación de régimen electoral. b) Los sometidos a la normativa sobre protección de materias clasificadas. c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes. d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36. e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio , Reguladora del Régimen del Personal Militar Profesional (Art. 2-2 y 2-3).

"privacidad" y la Intimidad" **[198]**. Distinción y alcances conceptuales que defiende *González Navarro* **[199]**) se plasma en el contexto de la norma jurídica, y sobre todo

en la circunstancia de que el derecho a la intimidad es la principal fuente de inspiración del texto garantista de los demás derechos y libertades fundamentales que persigue proteger la LORTAD en todo tratamiento informatizado de datos, tal como lo revela un sector de la doctrina ibérica [200].

---

(198) " *Nótese que se habla de la privacidad y no de la intimidad*: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona --el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo--, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo. Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona. Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos --datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado "dinero plástico", sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos-- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos" (E.M. núm. 1). Texto completo en AA. VV. *COLECCION DE DISCOS COMPACTOS DE ARANZADI*. Ed. Aranzadi, Pamplona, 1997.

(199) Previa a la transcripción de la E.M.núm. 1., el autor manifiesta: "Aunque suele pensarse que la protección de la privacidad tiene su fundamento en el derecho al honor y a la intimidad, y así parece resultar del artículo 18.4 , CE y de la misma exposición de motivos de la LORTAD que invoca expresamente este artículo, el verdadero fundamento de la específica protección de la privacidad se encuentra en el derecho al libre desenvolvimiento de la personalidad, un derecho que aunque no está específicamente mencionado en nuestra Constitución, es innegable que existe y está constitucionalmente protegido, como se prueba cuando se leen los artículos 14, 15, 16, 18.1, 20.1. b), 27.2, 38 y 44.1, todos los cuales pueden reconducirse a aquél". GONZÁLEZ NAVARRO, Francisco. COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y PROCEDIMIENTO ADMINISTRATIVO COMUN (Ley 30/92)., Ed. Civitas S.A., Madrid, 1997, pág. 697-698.

(200) Así se deduce del tratamiento y análisis que los diferentes autores ibéricos hacen de la LORTAD. A título de ejemplo, ORTI VALLEJO, Antonio. DERECHO A LA *INTIMIDAD E INFORMATICA*... Ob cit., ut supra. SOUVIRON, José M. *EN TORNO A LA JURIDIFICACION*... Ob. cit., ut supra. FAIREN GUILLEN, Victor. *EL HABEAS DATA Y SU PROTECCION ACTUAL*... Ob. cit. SARDINA VENTOSA, Francisco. *EL DERECHO A LA INTIMIDAD INFORMATIVA Y EL TRATAMIENTO DE DATOS PERSONALES PARA LA PREVENCION DEL FRAUDE*. En: Actualidad Informática Aranzadi. Núm. 25, Oct, Pamplona, 1997. LOPEZ DIAZ, Elvira. EL DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD. Ed. Dykinson, Madrid, 1996.

Pese a ello, la LORTAD, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter

personal para garantizar el honor, la intimidad personal y familiar de las personas físicas *y el pleno ejercicio de sus derechos* (art. 1); vale decir, del conjunto de derechos y libertades fundamentales previstos en la Constitución Española de 1978, aunque tanto en la praxis como en la teoría siga pesando el esquema de protección de la intimidad a través de las leyes protectoras de datos personales, y por su puesto, en la LORTAD.

Ahora bien, a nuestros efectos, analizaremos la visión iusinformática de la intimidad [201] tal y como hemos hecho con las demás normas relativas a la protección de los titulares de los datos. En tal virtud, abordamos y comentamos de la LORTAD, los siguientes temas: a) Las definiciones técnico-jurídicas; b) Los principios fundamentales aplicados a las fases del tratamiento informatizado de datos personales; c) Los órganos de protección de los datos personales; y, d) Las Inconstitucionalidades de la LORTAD, que afectan al tratamiento y proceso informatizado de datos.

4.4.1. DEFINICIONES TECNICO-JURIDICAS APLICABLES AL TRATAMIENTO INFORMATIZADO DE DATOS.

Con los antecedentes legislativos europeos (Alemania, Suiza, Francia, etc.) y comunitarios (básicamente de la Recomendación de la OCDE de 1980 y el Convenio Europeo de 1981), el Estado Español introdujo en su ordenamiento jurídico, una legislación homogénea, pero no plena en el tratamiento (informatizado o no) de datos de carácter personal de titularidad pública o de titularidad privada, con cierto retraso frente a la legislación estatal europea existente sobre la materia y sobre todo, con los avances tecnológicos del fenómeno TIC e informática [202], que se concretó en la L.O.

---

(201) En adelante se profundizará sobre el particular y sobre el estudio de la LORTAD, en las partes II, III y IV, por tal motivo, aquí haremos referencia a los comentarios y estudios puntuales que requiere el apartado 4 de ésta parte I, para exaltar la visión iusinformática del derecho a la intimidad y los demás derechos y libertades fundamentales previsto en la CE.

(202) La LORTAD, "se ha demorado quince años, pero finalmente está ya publicada", para destacar el epígrafe sobre "riesgos para los derechos de la personalidad que pueden derivar del acopio y tratamiento de datos por medios informáticos". Cfr. GONZALEZ N. Francisco. *DERECHO ADMINISTRATIVO ESPAÑOL*. Ed. Eunsa, Pamplona, 1994, p. 166. CASTELLS, sostiene: "La aparición de España de una red de tráfico de datos personales obrantes en registros públicos a comienzos de la década de los 90, reveló lo que una política puramente promocional del fenómeno informático, sin suficientes alertas en el plano cautelar, podía ocasionar, *Pérez Luño* ha mencionado "*la paradoja dramática"*, consistente en compensar el retraso en la incorporación al desarrollo tecnológico, con la vanguardia mundial en la piratería del "software", la delincuencia informática y las agresiones informáticas a la libertad".

5/1992, de 29 de Octubre conocida como LORTAD. Retraso morigerado, según se ha sostenido porque desde 1984, se conocía "un conjunto de normas heterogéneas que no siempre distinguían entre ficheros automatizados y ficheros convencionales" [203] y porque en nuestro criterio, se aplicaba teóricamente la Ley Orgánica núm. 1 de 5 de Mayo de 1982, relativa a la protección civil de los derechos del honor, la intimidad y el propia imagen, como norma jurídica subsidiaria en todos los asuntos relacionados con las intromisiones ilegítimas derivadas del uso de la informática (Disposición Primera Transitoria).

Este antecedente referencial legislativo, condujo a la LORTAD, a decantar y mejorar varias definiciones técnico-jurídicas aplicables al tratamiento informatizado de datos personales y la estructuración de procedimientos técnicos informáticos, a fin de hacerlas más inteligibles al operador jurídico, pero principalmente al juzgador que debe aplicar e interpretar la norma jurídica. Estas definiciones son: a) Datos de carácter personal, b) Fichero automatizado, c) Tratamiento de datos, d) Responsable del fichero, e) Afectado, y f) Procedimiento de disociación (art. 3-a) a f),).

Datos de carácter personal o simplemente datos personales, se considera cualquier información concerniente a personas físicas identificadas o identificables. Esta definición es idéntica a la prevista en el Convenio de 1981, por ello son válidas las observaciones realizadas en aquél aparte. Sin embargo, la LORTAD incluye entre sus definiciones la de "afectado", para indicar que se trata de una persona física titular de los datos que sean objeto del tratamiento informatizado, con lo cual abunda sin necesidad sobre el concepto de persona física (identificada o identificable) con el *inri* de que dicha persona no es en *strictu sensu* un *afectado,* sino un interesado, o mejor aún el titular de los datos personales o concernido en un tratamiento o procedimiento informatizado que tiene derechos y también deberes, no simplemente obligaciones o cargas como sugiere el concepto afectado. El titular de datos personales o interesado, contextua la idea de toda persona que tiene derechos subjetivos sobre la información

---

(203) El autor cita como ejemplos de dichas normas, entre otras, las siguientes: la LGT (arts. 111 y 112, modif. en 1985 y 1990), la ley 19 /1988 de 12 de julio, de auditoría de cuentas (arts. 13 y 14), y la ley 30/1984, de 2 de agosto, de Medidas para la reforma de la función pública (que prohibía registrar datos "sensibles" en los expedientes de personal). Refiriéndose ya específicamente a ficheros automatizados cabe citar la legislación electoral y la ley de la Función estadística pública, de 19802. Vid. GONZALEZ NAVARRO, Francisco. *DERECHO... Ob. cit.*, pág. 168.

relativa a sí misma, aún cuando tal información haya sido reunida por otras personas. Esta visión no sería posible si le anteponemos el calificativo de afectado para referirnos a esa misma persona.

Pero en lo que más destaca la LORTAD, dentro de este aparte de definiciones
es en los conceptos de "tratamiento de datos" informatizado y de "fichero automatizado" que el Convenio Europeo de 1981, había definido en forma general y sujeto a interpretaciones flexibles del operador jurídico con claras deficiencias, tal como se anotó puntualmente, sobre todo respecto al que llamó "tratamiento automatizado" de datos, excluyendo expresamente el tratamiento no informatizado de datos.

En efecto, la LORTAD, al definir Tratamiento de datos a las *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*, extiende el tratamiento a todo procedimiento técnico no informatizado y estructura el procedimiento de datos personales, a través de un *iter* compuesto de etapas o fases que encadenadas por un tratamiento informático, vale decir, con soportes y medios informáticos, electrónicos o telemáticos se dirigen a producir un dato informatizado, con el cual los responsables de la gestión, los titulares de los datos o los usuarios puedan desarrollar cualquier acción jurídico-técnica posible. v.gr. grabación, almacenamiento, bloqueo o interconexión. La definición de tratamiento de datos, destaca el iter informático que en su conjunto produce un proceso de igual carácter, es decir, un proceso informatizado de datos compuesto de fases o etapas, tales como las iniciales, de desarrollo y terminación. Estas fases, se estructuran con base en los principios fundamentales de la protección de los titulares de los datos personales.

Por su parte, al definir los *"ficheros automatizados"*, como *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*, excluye expresamente el concepto de

ficheros convencionales, manuales o no informatizados [204], con lo cual se establece

---

(204) Ob.ut supra cit., pág. 170

una contradicción conceptual con la de tratamiento de datos que incluye a los procedimientos técnicos informatizados y no informatizados . Sin embargo, se ha de interpretar que dicha definición no excluye sino que hace énfasis en el concepto técnico-jurídico de "automatizado " (o, mejor informatizado) y que algunos "usos" de los ficheros no informatizados se consideran incluidos, puesto que el ámbito de aplicación de la LORTAD, se extiende a los ficheros automatizados y no automatizados del sector público y privado, siempre que estén registrados en soportes físico compatible de tratamiento automatizado (art. 2).

En las definiciones anteriores se exaltan las etapas o fases del tratamiento informatizado de datos personales que conforman un procedimiento ibídem. En efecto, se destaca las fases de recolección, almacenamiento, registro, conservación y la comunicación (Emisión/transmisión y cesión) de datos personales. En tanto, que las acciones informáticas de revisión, actualización , rectificación, bloqueo y cancelación son originadas tras el ejercicio del derecho de información y acceso que tiene toda persona concernida con datos personales; vale decir, tras el ejercicio del derecho de *habeas data*.

Por ello, "la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia" (E.M. núm. 1).

El *Responsable del fichero*, se considera a la *persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento*. En esencia, contiene los elementos de la definición inmersos en el concepto de "autoridad controladora del fichero", previsto en el

Convenio Europeo de 1981, con la diferencia que en éste se especifican las funciones decisorias acerca de cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán a los ficheros, en tanto que la LORTAD, engloba y amplia el radio de acción, al expresar que dichas decisiones se extienden a "los contenidos y usos del tratamiento" y no simplemente de los ficheros, en particular.

Efectivamente, como lo sostiene el profesor *González Navarro* **[205]**, aparte de los dos sujetos (titular de los datos y el responsable del fichero), en el tratamiento de datos puede intervenir un tercer sujeto que es "el contratista o comisionista" que presta sus servicios de tratamiento informatizado de datos personales dentro de un procedimiento ibídem (art.27). Por su parte, la Ley Federal alemana de protección de datos personales (LFADP) extiende los efectos del principio de responsabilidad en el tratamiento de datos de los denominados "responsables del fichero" a las personas físicas o jurídicas, públicas o privadas que actúan como terceros en el mismo (v.gr. Oficinas de servicios informáticos), tanto de los deberes-derechos que estos tienen, como de las sanciones y la obligación de guardar la confidencialidad de los datos.

De otra parte, se considera *procedimiento de disociación*, a *todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable*. Este derecho-garantía para el titular de los datos personales y el Estado que debe regular, el tratamiento, uso y utilización de los mismos conforme a derecho, tiene aplicación práctica, así: En la distinción de *dato anónimo* **[206]** "*dato reservado*"**[207]**, comúnmente empleado en las normas jurídico-penales y ius-

---

(205) Este tercero, según el art. 27 no puede aplicar o utilizar los datos obtenidos con un fin distinto del que figura en el contrato de servicios, ni cederlos a otras personas ni siquiera para su conservación. Igualmente, una vez cumplida la prestación contractual, los datos personales deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se presten tales servicios, porque razonablemente se presumala posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años. Ob. ut supra cit., pág. 170.

(206) Los *datos anónimos*, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general. v.gr. como pueden ser los registros de la propiedad o mercantiles. Por ello, al determinar el ámbito de aplicación de la LORTAD, excluye de la aplicación del tratamiento informatizado de datos personales, los ficheros de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general (art. 2-a).

(207) De la interpretación doctrinal de los arts. 197.2 y 200 del Código Penal Español de 1995 (en adelante C.P.Esp.), se pueden deducir varios conceptos de dato reservado, a saber: 1. "Dato reservado es cualquier información concerniente a personas físicas identificadas o identificables cuyo conocimiento esta limitado a los usuarios del archivo, registro o fichero automatizado o convencional de acceso restringido. 2. Dato reservado es aquel que es indispensable libremente por terceros, requiriendose para ello autorización de su titular. 3. Dato reservado es aquel que potencialmente puede lesionar el derecho a la intimidad de su titular; en lo que respecta a las personas físicas, y cuyo descubrimiento o revelación debe incidir en la esfera "personal o familiar" de su titular..." Vid. BAJO FERNANDEZ, Miguel et all. *COMPENDIO DE DERECHO PENAL (Parte Especial).* Vol. II. Ed.Centro de Estudios Ramón Areces, S.A. Madrid, 1998, pág..201-202

administrativistas españolas. En efecto, a pesar de ser ambos datos de carácter personal, pregonables de una persona física, se diferencian en que éste último se predica única y exclusivamente de una persona identificada o identificable, so pena de desvirtuarse, y más aún, no haber existido, si alguna vez eso ocurrió. Tal es el caso, en el ámbito penal y más concretamente al referirse a los delitos contra la intimidad en el título X, Libro II del C.P.Esp., de 1995. Igualmente, en el ámbito administrativo, al referirse a las infracciones al tratamiento informatizado de datos previsto en la LORTAD (arts. 42 y 43).

De igual manera, tiene la aplicabilidad práctica el procedimiento de disociación cuando se refiere a los datos anónimos, a los efectos de hacerles perder la determinabilidad de una persona humana a la que le conciernen los datos de carácter personales. p.e., en los datos estadísticos, históricos, científicos, etc.

4.4.2. PRINCIPIOS FUNDAMENTALES APLICADOS A LAS FASES DEL TRATAMIENTO INFORMATIZADO DE DATOS PERSONALES

La institucionalización de "los principios reguladores de la recogida, registro y uso de datos personales" (E.M. núm.1) y demás fases o etapas del tratamiento informatizado de datos personales, tales como el almacenamiento, conservación y comunicación constituyen una garantía para el derecho al honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos (art. 1 *in fine*). Por ello, la existencia de los principios fundamentales del tratamiento informatizado de datos personales sólo encuentra validez, eficacia y presentación en la estructuración de sus fases o etapas, tales como la de recolección, almacenamiento, registro, conservación y comunicación de datos personales, reguladas por la LORTAD e inmersas en dentro del titulo II, sobre principios de la protección de datos: Calidad de los datos (art. 4), Derecho de información en la recogida de datos (art.5), Consentimiento del afectado (art.6), Datos especialmente

protegidos (art. 7), Datos relativos a la salud (art.8), Seguridad de datos (art. 9), Deber de secreto (art. 10) y Cesión de Datos (art.11) [208].

---

(208) El estudio y análisis de estos principios en las fases o etapas del procedimiento informatizado de datos se profundizará en la parte III y IV., de esta investigación. Por tanto, aquí sólo se referenciarán puntualmente

4.4.2. 1. FASE INICIAL DE RECOLECCIÓN DE DATOS.

En la *fase inicial de recolección de los datos,* se aplicarán los principios de *la congruencia y racionalidad,* así presentado por la E.M.núm. 1 de la LORTAD, para indicar con ello que sólo se podrán recoger datos personales para su tratamiento automatizado, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se haya obtenido (art.4.1).

Concordantemente con el anterior y por el *principio de calidad de los datos,* se prohíbe la recogida de los datos por medios fraudulentos, desleales o ilícitos (art. 4.7).

Por el principio del *consentimiento, o de autodeterminación* (art. 6), todo tratamiento informatizado de datos, y por su puesto, la recolección de los mismos, "requerirá el consentimiento" del titular, interesado o persona concernida, pues con él, se " otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del titular o interesado para que la recogida de datos sea lícita" (E.M.núm.1).

Sin embargo, no será preciso el consentimiento cuando los datos personales en los siguientes casos: a) Cuando se recojan de fuentes accesibles al público; b) cuando se recojan para el ejercicio de funciones propias de las Administraciones Públicas en el ámbito de sus competencias, c) Cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato (art.6-2). Más aún, podrá ser

revocado el consentimiento “cuando exista causa justificada para ello y no se le atribuya efectos retroactivos” (art. 6-3).

Por el *principio de información*, previo al principio del consentimiento y concomitante con el ejercicio de algunos derechos (v.gr. derecho de acceso a la información) y posterior con el ejercicio de otros, tales como el de habeas data, el titular de los datos personales puede informarse plenamente y en forma *a priori*, de qué datos suyos pudieran ser recolectados y sometidos a tratamiento informatizado.

Este principio fundamental que también es un derecho subjetivo de la persona concernida, porque le permite al titular de los datos “ser previamente informado de modo expreso, preciso e inequívoco” (art.5-1), cuando sean solicitados datos a él referentes y vayan a ser objeto de recolección y tratamiento informatizado. Quizá, por esto es uno de los principios de importancia capital para el pleno ejercicio del derecho de *habeas data* y los demás derechos y libertades fundamentales, y se aplica no sólo a la fase de recogida de datos sino al conjunto de fases o etapas del tratamiento informatizado de datos, como veremos cuando se interpreta hermenéuticamente el artículo 5 y 13 de la LORTAD. Su operatividad en esta fase, es como sigue:

El titular de los datos personales en la recogida de datos deberá ser informado de modo expreso, preciso e inequívoco [209]: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación (*habeas data*); e) De la identidad y dirección del responsable del fichero.

4.4.2.2. FASE DE ALMACENAMIENTO DE DATOS.

En la *fase de almacenamiento de datos* se aplicarán los siguientes: a) *El principio de adecuación, pertinencia y no excesibilidad de los datos* con relación al ámbito y las finalidades legítimas (art.1). Este principio que es válido para la recolección de los datos, lo es también para el almacenamiento, por cuanto, éste se

requiere para todo dato personal que sea sometido" a tratamiento" informatizado, y obviamente el almacenamiento posterior a la recogida de datos es una fase ineludible del tratamiento; b) El *principio del consentimiento* (art. 6-1), con igual razonamiento al precedente, se aplica este principio a la fase del almacenamiento de los datos, pues el consentimiento del titular se requiere durante todo el tratamiento; c) *El principio de veracidad de la información* (E.M.núm. 1). Los datos personales serán exactos y

---

(209) No será necesaria la información a que se refiere el apartado 1 del art. 5 de la LORTAD, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Esto como veremos luego, es objeto de un recurso de inconstitucionalidad ante el TC Español.

puestos al día de forma que respondan con veracidad a la situación real del titular (art. 4-3); d) *El principio de información* (arts 12, 4.6 y 13), que opera en todo el tratamiento informatizado de la información y que le permite al titular de los datos ejercer los derechos de acceso, habeas data e impugnación contra actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento o personalidad.

El principio del consentimiento en esta fase del tratamiento es importante, porque "otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes", niveles que "se refuerzan singularmente en los denominados *´datos sensibles´*, como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece *la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características*. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo

para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España" (E.M.núm. 1).

4.4.2.3. FASE DE REGISTRO DE DATOS.

En *la etapa del Registro de los datos*, se aplica: a) El *principio de exactitud y completud de los datos*. Si los datos personales registrados resultaren ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que los titulares de los mismos devenidas del ejercicio del derecho de *habeas data* -- lla- mados por la LORTAD "derechos de rectificación y cancelación" , artículo 15-- (art. 4.4) [2 10]. Así mismo, por aplicación de éste principio, podrán ser cancelados los datos "cuando hayan dejado de ser necesarios o pertinentes para la finalidad para cual hubieren sido recabados o registrados (art. 4.5).

Igualmente se aplicarán los principios del consentimiento, principio de información y el *principio de seguridad de datos*. Este último, como condición *sine cua nom* para el registro de datos, puesto que no se registrarán datos personales en ficheros informatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (art.9-2) [211].

Por *el principio de la confidencialidad de los datos*, aplicable a todo el tratamiento informatizado de datos, pero particularmente a las fases de registro, conservación y comunicación de datos, el responsable del fichero y quienes intervengan en "cualquier fase del tratamiento de los datos" personales están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo (art. 10).

4.4.2.4. FASE DE CONSERVACION DE DATOS.

En esta fase del tratamiento informatizado se aplicará: a) El *principio de la tem-poralidad de los datos*. Aplicable en dos formas: 1. no se serán conservados en forma que permita la identificación del titular de los datos durante un período superior al necesario para los fines en base a los cuales hubieran, salvo que deban mantenerse

---

(210) *Artículo 15. Derecho de rectificación y cancelación*.1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso. 3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario. 4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos..." Este artículo ha sido reglamentado por el art. 15 del Dec.1332/1994. En la parte III in fine, puntualizaremos sobre esto.

(211) En la parte III, destinaremos un aparte especial para el estudio de las aplicaciones, soportes y medios informáticos, electrónicos o telemáticos utilizados en el tratamiento informatizado de los datos personales. Legislativamente el Estado Español ha dictado recientemente un Real Decreto núm. 263/1996, de 16 de Febrero, por el cual "Regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado", reglamentario del art. 45 de la Ley 30/1992, de 26 de noviembre y aplicable a las Administraciones Públicas Generales del Estado.

en su integridad atendiendo al valor histórico que los datos puedan tener de conformidad con el ordenamiento jurídico vigente. (art. 4.5 *in fine*); y 2. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el titular de los mismos (art.15.5).

b) Por el *principio de seguridad de los datos*, el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural (art. 9-1).

c) Por *el principio de tutela de derechos del titular de los datos*, integrado por los anteriores principios y los referentes al derecho de *habeas data*, el titular podrá ejercer el derecho de acceso, a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes --art. 14-3-[212].

Igualmente son aplicables los principios del consentimiento y principio de información, los cuales son deben observarse en todo procedimiento o tratamiento informatizado de datos.

4.4.2.5. FASE DE COMUNICACION DE LOS DATOS.

Esta fase del tratamiento informatizado se estructura en la emisión y transmisión de los datos personales, a través de soportes y medios informáticos, electrónicos o telemáticos idóneos para la comunicación o la cesión de los mismos. Se entiende por *cesión de datos*, toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero; y sobre todo, la actividad

---

(212) *LORTAD. Art. 14. Derecho de acceso*."1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados. 2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos".

de interconexión con otros ficheros y la comunicación de los datos realizada por una persona distinta del titular de los datos personales.

En consecuencia, serán aplicables los principios de consentimiento, información, confidencialidad y seguridad de los datos, por tener aplicabilidad en todas las fases del tratamiento informatizado.

Por *el principio del consentimiento o autodeterminación* del titular de los datos, la LORTAD,

> *"se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completa el principio del consentimiento, exigiendo que, al procederse la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona (art. 8.2) y del Convenio 108 del Consejo de Europa (art. 9.2), que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla." (E.M. núm. 2)*

La regla general establecida en la LORTAD referente a la cesión de datos, es que con objeto del tratamiento informatizado de datos personales sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones

legítimas del cedente y del cesionario con el previo consentimiento del titular de los datos (art.11-1). El consentimiento debe reunir los requisitos de forma y de fondo establecido en la LORTAD para que tenga aplicabilidad en la fase de cesión, de lo contrario podrá ser anulado, revocado o incluso no requerido, si previamente se aplicado procedimiento de disociación a los datos [213].

Sin embargo, como excepciones a la regla se establecen los siguientes casos: a) Cuando una Ley prevea otra cosa; b) Cuando se trate de datos recogidos de fuentes accesibles al público; c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros.

---

(213) Art. 11-3, LORTAD,. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente. 4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable. 5. El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la LORTAD. 6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique; d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas; e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos de diversidad de competencias y creación de ficheros; y , f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero informatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad (art. 11-2).

El *principio de libre circulación de datos,* aplicable a las comunicaciones de datos personales denominado por la LORTAD, como “movimiento internacional de datos” (art. 32). En este punto, la Ley traspone la norma del artículo 12 del Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con *el libre flujo de los datos,* que constituye una auténtica necesidad de la vida actual de la que las transferencias

bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias. (E.M. núm. 4 *in fine)*

4.4.3. ORGANOS DE PROTECCIÓN DE LOS DATOS PERSONALES.

La LORTAD establece como órganos de la protección de los datos personales a los siguientes: a) La Agencia de protección de datos, que como organismos de régimen jurídico *sui géneris* cuenta con un Director asesorado con un "Consejo Consultivo"; b) El Registro de protección de datos, como órgano integrado a la Agencia; la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia (art. 11-3, R.D.núm.428/1993, de 26 de Marzo).; y c) Organos de protección de datos de las Comunidades autónomas [214].

4.4.3.1. LA AGENCIA DE PROTECCIÓN DE DATOS.

La Agencia de Protección de Datos Española, es la entidad pública, con personalidad jurídica propia y plena capacidad pública [215] y privada [216], que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones, con un régimen jurídico *sui géneris* (integrado por la LORTAD, un Estatuto propio dictado por el Gobierno R.D.núm.428/1993, de 26 de Marzo [217]; así como, la disposi-

---

(214) A efectos prioritarios de la investigación nos referiremos a la Agencia y el Director de Protección de Datos, pues los otros organismos han sido puntualmente tratados por Francisco González Navarro, José María Souvirón, Fairen Guillen, Castells Arteche, en sus diferentes obras ut supra citadas. Sin embargo, destaque-mos

que *el Consejo Consultivo* que asesora al Director de la Agencia, es "un órgano de apoyo definido por los caracteres de colegiación y representatividad, en el que obtendrán presencia las Cámaras que representan a la soberanía nacional, las Administraciones Públicas en cuanto titulares de ficheros objeto de la presente Ley, el sector privado, las organizaciones de usuarios y consumidores y otras personas relacionadas con las diversas funciones que cumplen los archivos informatizados" (M.E.núm 5).

(215) En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la LORTAD y sus normas de desarrollo (El Real Decreto 428/1993, de 26 de Marzo, reglamentario de la LORTAD, conocido como Estatuto de la Agencia de Protección de Datos)., la Agencia actuará de conformidad con la ley de Pro-cedimiento Administrativo (antes LPA.; hoy, LRJAP: Ley de Régimen Jurídico de las Administraciones Públicas y procedimiento administrativo común. Ley 30/1992, de 26 de Noviembre)-- Art. 34.3 LORTAD--. Vale decir, que a este tipo de funciones se aplica un régimen jurídico de derecho público, donde la LORTAD es la norma especial y la LRJAP, es la norma subsidiaria para llenar lagunas y vacíos normativos de aquélla.

(216) En su adquisiciones patrimoniales y contratación estará sujeta al Derecho privado. Este dual régimen jurídico (público y privado) aplicable por la Agencia de Protección de datos es lo que caracteriza un régimen sui géneris, además de la condición de entidad (por "Ente") de derecho público con funciones públicas y privadas a la vez e independiente de las Administraciones Públicas.

(217) El R.D.núm. 428 /1993, lo concreta normativamenta así: "Artículo 2. *Régimen jurídico*.1. La Agencia de Protección de Datos goza de personalidad jurídica propia y plena capacidad pública y privada. 2. La Agencia de Protección de Datos se regirá por las disposiciones legales y reglamentarias siguientes: a) El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. b) El presente Estatuto y las demás disposiciones de desarrollo de la Ley Orgánica 5/1992. c) En defecto de las anteriores, y para el ejercicio de sus funciones públicas, las normas de procedimiento contenidas en la Ley 30/1992, de 26 de noviembre, "Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común". d) Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación. e) Cuantas otras disposiciones resulten de aplicación. 3. La Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia. 4. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

ción tipo "cajón de sastre" **[218]** del art.6.5. LGP). La Agencia, tiene como objetivo prioritario velar por el cumplimiento de la legislación en materia de protección de datos personales informatizados en España, pero particularmente, la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de octubre, de *Regulación del Tratamiento Automatizado de los Datos de Carácter Personal* y los derechos y libertades fundamentales e intereses legítimos implicados en ella.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un numerus clausus de causas de cese.

La Agencia de Protección de datos tendrá como funciones, las siguientes:

1. *Funciones de control y vigilancia*:

La Agencia de Protección de datos tendrá como funciones el velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos. Así mismo:

a) Ejercerá el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen (SIS) (art. 10 R.D.428/1993), b) Velará por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicará y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información adicional que determine el Director (LORTAD, art. 36-j., art.7 R.D.428/1993), c) ejercerá el control de la observancia de lo dispuesto en los

---

(218) Así lo califica el profesor *González N.*, al "art. 6.5 de LGP --Ley General de Presupuesto, del cual dice-- quedará en la historia de derecho público como ejemplo de lo arriesgado que resulta al poner en manos de los adoradores del Poder preceptos tipo "cajón de sastre". Con base esa norma se van aumentando los organismos autónomos o independientes que buscan el camino de la "libertad" (entiéndase: de la reducción al máximo de cualquier forma de control). GONZALEZ NAVARRO, Francisco. *COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LAS ADMINISTRACIONES PUBLICAS Y EL PROCEDIMIENTO ADMINISTRATIVO COMUN.*, 1a., ed., Ed. Civitas S.A., Madrid, 1997, pág.705.

artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial: i) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadísticos. ii) Dictaminará sobre los procesos de recogida y tratamiento automatizado de los datos personales a efectos estadísticos. iii) Informará sobre los proyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley de la Función Estadística Pública. iv) Dictaminará sobra las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos (art. 7 R.D.428/1993).

Igualmente, tendrá como funciones de control y vigilancia: a) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias (art.36-b LO 5/1992), b) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LORTAD (art. 36-c LO 5/1992), c) Atender las peticiones y

reclamaciones formuladas por las personas afectadas (art. 36-d, LO 5/1992), d) Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la presente Ley (art. 36-f, LO 5/1992) y, e) Ejercer la potestad sancionadora en los términos previstos por el título VII de la LORTAD, (art.36-g. LO 5/1992, o "proceso descodificador"(por *decodificador*) establecido por la LRJPA [219].

2. *Funciones de Relaciones con los titulares de los datos*:

a) La Agencia informará a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social (art. 4-1 R.D.428/1993) y, b) La Agencia atenderá las peticiones que le dirijan los afectados y resolverá las reclamaciones formuladas por los mismos, sin perjuicio de las vías de recurso procedentes (art. 4-2. R.D.428/1993).

3. *Funciones de Cooperación y Asistencia entre organismos*:

a) La Agencia cooperará con los organismos internacionales y órganos de las

---

(219) Ibídem., pág. 706.

Comunidades Europeas en materia de protección de datos (art 9-1.R.D.428/1993), b) prestará asistencia a las autoridades designadas por los Estados parte en el Convenio Europeo de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos de garantizar el derecho de información de los titulares de los datos en dicho tratamiento (art 9-2. R.D.428/1993) y, c) colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la LORTAD (art.5 R.D.428/1993)

4. *Funciones de presentación de Memorias e informes*:

a) La Agencia de Protección de Datos redactará una Memoria anual, la cual será remitida por el Director al Ministro de Justicia, para su ulterior envío a las

Cortes Gene- rales, sobre la aplicación de la LORTAD y demás normas reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre el funcionamiento de la Agencia: i) Una relación de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos, ii) Un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos. 3. Un análisis y una valoración de los problemas de la protección de datos a escala nacional (art. 6. R.D.428/1993) y, iii) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal (art.36-e, LO.5/1992); c) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley (art. 36-h. LO 5/1992); y, d) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones (art.36-i, LO 5/1992).

5. *Funciones de Inspección*:

La Agencia de Protección de datos podrá Inspeccionar los ficheros tanto de titularidad público como de titularidad privada, recabando cuantas informaciones precise para el cumplimiento de sus cometidos. A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior, tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Así mismo, estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas (art.39 LO 5/1992).

4.4.3.2. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS.

El *Director de la Agencia de Protección de Datos,* dirige la Agencia y ostenta su representación. Prioritariamente el Director hará cumplir y cumplirá todo lo atinente a la legislación sobre tratamiento informatizado de datos personales y en

su carácter de funcionario ejecutor de las políticas, recomendaciones y sugerencias de la Agencia de Protección de Datos, velará y controlará el ejercicio de los derechos de información, *habeas data* (acceso, actualización, rectificación , bloqueo y cancelación de datos) y el pleno de derechos y libertades fundamentales e intereses legítimos.

El Director será nombrado, de entre quienes componen el consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Cesará antes de la expiración del período, por las siguientes causas: 1. A petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo; 2. Por incumplimiento grave de sus obligaciones, 3. Por incapacidad sobrevenida para el ejercicio de su función, y, 4. por incompatibilidad o condena por delito doloso.

El Director de la Agencia, tiene una gama variopinta de funciones, tales como las de Dirección [220], de Gestión [221] y designación [222], que apuntan a determinar

---

(220) A título de ejemplo: "Dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial: a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos. b) Requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo. c) Resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados. d) Autorizar transferencias temporales o definitivas de datos que hayan sido objeto de tratamiento automatizado o recogidos a tal efecto, con destino a países cuya legislación no ofrezca un nivel de protección equiparable al de la Ley Orgánica 5/1992 y el presente estatuto..." (Art. 12 R.D.428/1993).

(221) A título de ejemplo: a) Adjudicar y formalizar los contratos que requiera la gestión de la Agencia y vigilar su cumplimiento y ejecución. b) Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia (art. 13 Ibídem).

(222) Designará a dos (2) representantes para la autoridad de control común de protección de datos del Sistema de Información Schengen (art.10-2, R.D.núm.428/1993).

que su cargo se desempeña con dedicación absoluta, plena independencia y total objetividad, y por ello no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna (art. 16 R.D.428/1993). Gozará de los mismos honores y tratamiento que los subsecretarios del Estado (art. 14-2 Ibídem).

4.4.4. INCONSTITUCIONALIDADES DE LA LORTAD, QUE AFECTAN EL TRATAMIENTO Y PROCESO INFORMATIZADO DE DATOS.

Existen actualmente varios recursos de inconstitucionalidad en contra de la LORTAD (L.O. 5/1992, Oct. 29), los cuales han sido presentados por el

Defensor del Pueblo [223], El Parlamento Catalán [224], El Consejo Consultivo de la Generalidad

---

(223) EL DEFENSOR DEL PUEBLO interpuso el núm. 219/1993 contra el art. 19-1 de la LORTAD [”Cesión de datos entre Administraciones Públicas. 1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de sus competencias, *salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso”*]; y el art.22-1 de la LORTAD [Otras excepciones a los derechos de los afectados. 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de *las funciones de control y verificación de las Administraciones Públicas* de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o *a la persecusión de infracciones* penales o *administrativas”* y el art. 22-2 Ibídem [2. *Lo dispuesto en el art. 14 y en el art. 1 del artículo 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección.* Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas”]. Las partes en cursiva son las cuestionadas constitucionalmente. Argumento principal: Quebrantamiento del principio de reserva de ley (art. 53.1 CE). Anotaciones referenciales sobre la materia, en: CASTELLS ARTECHE, José M. *DERECHO A LA PRIVACIDAD Y PROCESOS INFORMATICOS: ANALISIS DE LA LORTAD*. R.V.A.P. Bilbao, 1997, pág. 253

(224) EL PARLAMENTO DE CATALUÑA EN 1993, propuso recurso de inconstitucionalidad contra los arts. 24 LORTAD [Artículo 24. Notificación e inscripción registral. 1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar. 3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero automatizado si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos]; Art. 31 LORTAD [Artículo 31. Códigos tipo. 1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección

de Cataluña [225] y el Partido Popular [226], ante el Tribunal Constitucional Español que aún permanecen irresolutos y que inciden sobre la columna vertebral del tratamiento y proceso informatizado de datos personales y la distribución competencial en estas materias entre el Estado y las Comunidades Autónomas, con lo cual se transgrede el llamado “Bloque de Constitucionalidad” previsto en el Ordenamiento Jurídico Español. Sin embargo, a los efectos de esta investigación nos detendremos en el análisis de los recursos de inconstitucionalidad a los artículos de la LORTAD que vulneran los *principios y derechos fundamentales* de los

titulares de los datos personales en el tratamiento y proceso informatizado, pues estos, como apunta el profesor *Morales*

---Continuación nota 224--

de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas]; Art. 40.1 Ibídem [Artículo 40. Organos correspondientes de las Comunidades Autónomas. 1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido]; y Art. 40.2. Ibídem [2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos]. Argumento básico: Desconocer el marco de distribución competencial entre el Estado y las Comunidades autónomas infringiendo así el llamado bloque de constitucionalidad. Distribución competencial que no abarca la competencia exclusiva del Estado en materia de derechos y libertades fundamentales, previstos en el art. 149.1 CE.

(225) EL CONSEJO EJECUTIVO DE LA GENERALIDAD DE CATALUÑA interpuso recurso de incons titucionalidad contra los arts. 24, 31, 39, 40.1 y 2, y la disposición final tercera de la LORTAD [Tercera. Preceptos con carácter de Ley ordinaria. Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley ordinaria]. Los Recursos del Parlamento y Consejo Consultivo de la Generalidad Catalana, como sostiene *Souvirón*, están basados en un dictamen del Consejo Consultivo de la Generalidad, de 23 de diciembre de 1992, según el cual resultarían inconstitucionales los arts. 5.2, 19.1, 20.3, 21.1, 22, 24, 31 y 40.1 y 2 LORTAD, reivindican la competencia de las Comunidades Autónomas sobre los ficheros de titularidad privada y los de la Administración Local que la LORTAD atribuye a la Administración del Estado". Vid. SOUVIRON, José María. *EN TORNO A LA JURIDIFICACION DEL PODER.... Ob. cit.*,pág. 142.

(226) EL GRUPO POPULAR interpuso recurso de inconstitucionalidad contra los artículos 6.2 [Artículo 6. Consentimiento del afectado. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato] y los arts. 19.1, 20.3 [Artículo 20. Ficheros de las Fuerzas y Cuerpos de Seguridad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.], arts. 22.1 y 22.2 "y los demás que procedieren por conexión"

.

Prats **[227]**, tienden a *rebajar incluso los mínimos de tutela que marca el Convenio Europeo de 1981 en la informatización y manejo de los datos personales en el ciclo operativo de los bancos de datos.*

Sea lo primero, decir que muchos de los recursos de inconstitucionalidad que hoy permanecen *sub judice* ante el Tribunal Constitucional, se ven tocados en su esenciaantes y después de expedida y puesta en vigor la LORTAD, por normas

comunitarias europeas que regulan el tratamiento informatizado de los datos personales y la protección de las personas físicas en el pleno ejercicio de los derechos y libertades fundamentales e intereses legítimos con relación a aquél.

En efecto; la primera, es el Convenio del Consejo de Europeo de 1981, ratificado por España, mediante Instrumento de 24 de Enero de 1984, el cual forma parte del Ordenamiento jurídico interno español (art.96.1 CE. Publicado en el BOE, Nov.15/1985); y además, constituye un instrumento jurídico con alcance interpretativo de los derechos y libertades fundamentales reconocidos por la CE (art. 10.2) , y particularmente de los derechos al honor, a la intimidad personal y familiar "y el pleno ejercicio de sus derechos" --art.18.4 CE-- (STC 254/1993, de 20 de Julio. BOE del 18 de Agosto), cuando se aplica al tratamiento informatizado de datos personales, ante la ausencia legislativa de una norma jurídica en vigor en España que regulara dicho tratamiento en la fecha de ocurrencia de los hechos y de presentación de la demanda ante los Tribunales Contencioso-administrativos e incluso de la fecha de presentación del recurso de amparo ante el Tribunal Constitucional de España [228].

La segunda, consistente en la transposición de la normativa comunitaria al ordenamiento jurídico español, básicamente de dos Directivas Comunitarias que

---

(227) MORALES PRATS, Fermín. COMENTARIOS A LA PARTE ESPECIAL DEL CODIGO PENAL. En: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio. Ed. Aranzadi, Pamplona (Nav.), 1996, págs.309 y ss.

(228) Los hechos del que se ha conocido en la doctrina española como el "Caso Olaverri", se inician por la petición del Sr. Francisco Javier, en febrero de 1986, dirigida al Gobernador Civil de Guipuzcua con miras a proteger sus derechos fundamentales de la intimidad y la imagen (F.J.2 STC.254/1993). Petición que se concretaba en solicitar al Gobierno Civil si existían o no datos de carácter personal que le conciernan en el fichero informatizado que la Administración del Estado manejaba o gestionaba. Los Tribunales Contencioso-administrativos , desestimaron los recursos de D. Francisco Javier, básicamente porque "el Convenio (Europeo de 1981) no era de aplicación directa, siendo preciso el complemento de la actividad legislativa y reglamentaria interna para la aplicación práctica de sus disposiciones en España" (F.J.1 Ibídem), lo cual obligó al petente a recurrir ante el Tribunal Constitucional en recurso de amparo de sus derechos fundamentales.

aluden al tratamiento informatizado de datos personales y su incidencia con los derechos y libertades fundamentales reconocidos en la CE. Estas son: a) la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y, b) la Directiva 97/66/CE, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas. Transposición

normativa que el caso del derecho español, deberá haberse verificado el 28 de Octubre de 1998, al menos para la Directiva 95/46/CE, tal y como lo prevé aquélla en las disposiciones finales (art. 32) [229] .

En consecuencia, atendiendo a la estructura de estudio y análisis que venimos haciendo de las normas estatales y comunitarias que regulan el tratamiento y proceso informatizado de datos personales, haremos mención a los recursos de inconstitucionalidad a los artículos de la LORTAD que afectan a los principios de información y los componentes del derecho de *habeas data* (acceso, actualización, rectificación, bloque y cancelación de datos); el principio del consentimiento en las fases o etapas de recolección, de almacenamiento, de registro y comunicación (prioritariamente en la "cesión de datos") de datos personales; y, el principio de reserva de ley para el ejercicio, garantía y protección de derechos y libertades fundamentales (art.53-1 CE). Principios fundamentales obviamente contenidos en derechos de igual rango que se ven vulnerados por la actual regulación de la LORTAD, aunque hay quienes sostienen [230], que la inconstitucionalidad de la LORTAD, no se

---

(229) La Directiva 95/46/CE. "Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste-eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento" (Considerando 69). Texto en WWW.CC.CEC(Database CELEX).

(230) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, Antonio. *SOBRE LA INCONSTITUCIONALI DAD DE LA LEY DE PROTECCION DE DATOS INFORMATICOS.* En: Revista Actualidad Aranzadi Núm. 8 de Julio, Pamplona, 1993, pág. 6.

debe a *una escasa o deficiente regulación de los derechos del ciudadano o de las garantías reconocidas para el pleno ejercicio de los mismos, sino de las múltiples excepciones que dentro de dicho texto se prevén para unos y otras.* Sin embargo, son de tanta envergadura las excepciones que vacían de contenido, o más aún desvirtúan la esencia o núcleo del derecho que las contiene.

4.4.4. 1. PRINCIPIO FUNDAMENTAL DE LA INFORMACION Y EL

***HABEAS DATA*.**

A. Inaplicación del derecho a la información y el ejercicio del *habeas data (art.5*.3, en relación con el art. 5-1).

Se ha sostenido, que el derecho a la información y el derecho de *habeas data* aplicables al tratamiento informatizado de datos y previstos en la LORTAD (arts. 5 y 13 y 14 a 16, respectivamente) con carácter *in genere* a la totalidad de las fases o etapas del ciclo informático de las bases de datos personales, constituyen además principios fundamentales de expresa observancia por quienes están involucrados en estos procesos de características técnico-jurídicas especiales, tal y como son, los informatizados de datos personales.

El principio-derecho a la información que tienen los titulares de los datos constituye una garantía *a priori y* concomitante a un tratamiento informatizado de datos por quienes estén involucrados en dicho proceso (especialmente los responsables de los ficheros y/o autoridades competentes en dicho proceso), pero particularmente en la fase inicial de recolección de los datos personales, deberán previamente informar de modo expreso, preciso o inequívoco, a los interesados, acerca: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos, d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación y, e) De la identidad y dirección del responsable del fichero (Art.5-1).

Sin embargo, se cuestiona la constitucionalidad del art.5-3, que prevé excepciones a la regla general del art.5-1, cuando expresa: "*No será necesaria la información a que se refiere el apartado 1, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban*".

Estas excepciones al derecho de la información y el ejercicio de los derechos de *habeas data* (acceso, rectificación y cancelación), plasmados en la norma recurrida ante el Tribunal Constitucional Español, desvirtúa y vacía de contenido la regla general, basado en una cláusula general indeterminada, asentada en criterios

vagos (*la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban* [231]) y utilizada para recortar arbitrariamente uno de los derechos esenciales del *´habeas data´* del ciudadano, reconocido en el art. 18.4 [232], en "cuanto que habría un grave peligro para la intimidad ... (y el pleno ejercicio de los derechos del ciudadano previstos en la CE, con lo cual también se vulnera) el artículo 9.3 de la Constitución, que garantiza la *seguridad jurídica* [233].

Igualmente se endilga razones de inconstitucionalidad al art. 5-3, no sólo por rebajar el mínimo de garantías denominadas "complementarias para la persona concernida", prevista en el art. 8 Convenio Europeo de 1981, de parecida redacción al art.5.1 LORTAD (aunque mucho más recortado que el del Convenio, lo cual *per se* ya es un motivo de desconocimiento del "mínimo irreductible" de derechos del titular), sino por desconocer flagrantemente el marco de las causales *numerus clausus*, que como excepciones taxativas se plantean a los derechos de información y al ejercicio del derecho de habeas data en el art. 9 del Convenio Europeo de 1981., y consistentes en la Seguridad del Estado, la Seguridad Pública, los intereses monetarios del Estado o la represión de infracciones penales, así como la protección de la persona concernida y los derechos y libertades de otras personas. Incluyo se desconoce el marco de las que el Convenio de 1981, denomina "restricciones" (que jurídica y strictu sensu no son "excepciones") a los derechos de información y de habeas data (que abarca además a los derechos de borrado o de recurso, si fuere el caso), para "los ficheros automatiza-

---

(231) Según, *López G.*, "Estos términos conceden al funcionario o empleado encargado de suministrar los datos, un ámbito de discrecionalidad tan amplio que se confunde con la arbitrariedad y que hace perder todo sentido a las garantías establecidas en el apartado 1 del art. 5". LOPEZ GARRIDO, Diego. *ASPECTOS DE INCONSTITUCIONALIDAD DE LA LEY ORGANICA 5/1992, DE 29 DE OCTUBRE*. En: Revista de Derecho Político. Universidad nacional de Educación a Distancia, UNED. Núm. 38, Madrid, 1993, pág. 24.
(232) MORALES PRATS, Fermín. COMENTARIOS A LA PARTE... Ob.cit., pág.309 y ss.
(233) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 24.

dos de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas" (art. 9-3).

B. Excepciones a los derechos de los titulares de los datos en los Ficheros de Titularidad pública (art. 22.1., en relación con el art. 5-1 y 5-2; y, art. 22.2, en relación con los arts. 14 y 15-1).

Por su parte, se considera inconstitucional el art. 22.1 de la LORTAD, que inaplica el art. 5-1 y 2 de la misma Ley Orgánica, contentivos de los derechos a la información y de habeas data que tiene el titular de los mismos, en la fase o etapa inicial de recolección de datos personales informatizados e incluso no informatizados (al hacer mención "cuestionarios u otros impresos para la recogida de datos"), según dice el art. 22.1, " cuando la información al titular impide o dificulte gravemente el cumplimiento de las *funciones de control y verificación de las Administraciones Públicas* o cuando afecte a la Defensa Nacional, a la seguridad Pública o a la persecución penales o *administrativas"*.

Esta inaplicación legislativa del derecho a la información, que no es una excepción jurídicamente hablando, sino una abrogación normativa del propio legislador y que en la doctrina ibérica se ha entendido como una "denegatoria" de aquél derecho, basados en causales indeterminadas, abstractas y vaporosas, como son el impedimento o dificultad grave del cumplimiento de funciones gubernamentales. Aunque se expresa que dichas funciones son las "control y verificación de las administraciones Públicas", estas son tan amplias como indeterminadas, máxime cuando un grupo amplísimo de las funciones gubernamentales tienen por objeto las actividades controladoras o verificadoras de actos, hechos, acciones o omisiones tanto subjetivas como objetivas de los ciudadanos, de los funcionarios y la propia Administración. La Administración en este caso carece de límites claros y precisos que le obliguen a dar prevalencia al derecho que tiene el ciudadano a ser informado de las garantías en la recogida de datos, lo que sería incompatible con el principio de seguridad jurídica y de interdicción de la arbitrariedad (art.9.3 CE), o incluso contrario al art. 10.2 y 53.1, ya que esas excepciones no respetan el contenido esencial ni una adecuada interpretación conforme al Convenio de 1981, del derecho a la intimidad personal y familiar y el pleno ejercicio de los demás derechos previstos en la CE **[234]**.

---

(234) QUILEZ AGREDA, Ernesto y otro. Ob. ut supra cit., pág. 7.

Igualmente se reputa como inconstitucional, el art.22.1, porque la mencionada inaplicación legislativa, se extienda a causales que incluso desbordan el régimen de excepciones y restricciones previsto en el Convenio Europeo de 1981, cuando deja de aplicar el art. 5-1 y 5-2, a "la persecución... administrativas", causal ésta que junto a las anteriores, se prevén en el art.9, como "excepciones a las garantías de" aquél, según lo sostiene *López Garido*, se vulnera así, el "contenido

esencial de los derechos protegidos en el art.18.4 CE" (STC 11/1981, de 8 de abril [235]).

Con mayor incidencia, el art. 22.2 LORTAD, se reputa inconstitucional, porque éste inaplica lo dispuesto en el art. 14 y 15-1, es decir, que desconoce el ejercicio de los derechos estructurales del derecho de *habeas data* (acceso, rectificación y cancelación), que esta garantizado por la CE, como por el Consejo de Europa de 1981, para todo ciudadano o titular de los datos personales. La inaplicación del derecho de *habeas data*, opera, según la norma cuestionada por inconstitucionalidad, "si ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado (por interesado) hubieran de ceder ante razones de *interés público* o ante *intereses de terceros* más dignos de protección".

La inaplicación legislativa al ejercicio del derecho de habeas data, "constituye una cláusula indeterminada que posibilita la arbitrariedad frente al ejercicio del *habeas data*, y debe reputarse vulneradora de lo dispuesto en el art.9 del Convenio del Consejo de Europa y, por ende, del art. 18.4 CE" [236].

Igualmente, es inconstitucional la norma jurídica en la utilización de términos"intereses de terceros", por ser excesivamente amplios e indeterminados y

---

(235) Citada por López Garrido, la cual expresa: "Constituyen el contenido esencial de un derecho subjetivo aquellas facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a este tipo y tiene que pasar a quedar comprendido en otro desnaturalizándose.... Se puede entonces hablar de una esencialidad del contenido del derecho para hacer referencia a aquella parte del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección... Se entiende por contenido esencial aquella parte del contenido de un derecho sin la cual éste pierde su peculiaridad, o dicho de otro modo, lo que hace que sea recognoscible como derecho perteneciente a un determinado tipo. Es también aquella parte del contenido que es ineludiblemente necesaria para que el derecho permita a su titular la satisfacción de aquellos intereses para cuya persecusión el derecho se otorga". LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 18

(236) MORALES PRATS, F. Ob. cit., pág.309 y ss.

rebasar las excepciones previstas en el art. 9 del Convenio Europeo que justifica la excepción a las garantías establecidas cuando se tomen medidas necesarias en una sociedad democrática para la *protección de la persona concernida y de los derechos y libertades de otras personas*. Parece claro, como sostiene *López Garrido* [237], que los términos "derechos y libertades" son mucho más concretos y específicos que los

términos “intereses” que emplea el art. 22.2. Más aún, son términos difusos y abstractos.

4.4.4. 2. PRINCIPIO FUNDAMENTAL DEL CONSENTIMIENTO Y EL *HABEAS DATA*.

A. Tratamiento informatizado de datos personales considerados sensibles, aún con el consentimiento --expreso y escrito o meramente manifestado-- (Art.7 en relación con el art. 6.1) .

La expresión exterior del consentimiento humano (en forma escrita o tácita), constituye el basamento de todo proceso informatizado de datos personales (generales o “sensibles”) en el ordenamiento jurídico ibérico sobre la materia. Por ello, se ha elevado a rango de principio fundamental en la LORTAD, principio del consentimiento que rige para todo tratamiento informatizado y en todas sus fases (recolección, almacenamiento, registro, conservación y comunicación) constitutivas de proceso ibídem, aunque a veces, la propia ley acentúa su énfasis de protección a alguna de las fases por el acrecentamiento del riesgo o vulnerabilidad que aquellas representan frente a las acciones que pretenden desvirtuarlas tras el desconocimiento de derechos y libertades fundamentales, tanto por particulares como por personas físicas o jurídicas de derecho público. v.gr. En el almacenamiento de datos sensibles (art. 4-2): El caso de la huelga en la “RENFE” (Ferrocarriles de España) y la nómina del personal [238].

---

(237) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 31-33.

(238) Vid. Sentencia del Tribunal Constitucional (TC), 11/1998, de 13 de enero. La empresa estatal RENFE, en el mes de mayo de 1994, retiene una cantidad del salario de un trabajador de la empresa, por la su puesta participación en los paros de los meses anteriores. Retención que se hace de la nómina informa- tizada (base de datos) que gestiona la empresa. El trabajador agota todas las instancias jurisdiccionales hasta incoar el Recurso de Amparo ante el TC. Ante el TC, considera que se le han vulnerado la libertad sindical (art. 28 CE), en conexión con los arts. 16.1, 18.1 y 18.4 CE, así como los artículos 4.2 y 7.1, LORTAD. El TC, en su fallo analiza los planteamientos, y sobre todo en lo que aquí nos interesa, los quebrantamientos del art. 18.4 CE y los artículos de la LORTAD, con base en los planteamientos vertidos en otro caso y fallo ilustre sobre la materia: la Sent. 254/1993, para concluir que efectivamente dichos textos normativos se han visto vulnerados por la actuación de la empresa recurrida. Un análisis más detallado de esta sentencia se hace en el punto 3 de la parte I., de esta investigación.

Por su parte, el art. 6 del Convenio Europeo de 1981, proscribe todo proceso informatizado de datos personales considerados sensibles (relativos a la vida sexual, el origen racial, la salud, las creencias, la ideología, las opiniones políticas, las convicciones religiosas u otras convicciones), a menos que el derecho interno prevea

garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal
referentes a condenas penales.

Pues bien, la LORTAD en el art. 6 y 7, al permitir el tratamiento informatizado de datos personales sensibles, aún con ciertas garantías que se consideran insuficientes a la vista de las normas universales, y en especial del Convenio de 1981, se estima que no se halla dentro de ese margen exceptivo de "garantías apropiadas" exigido por el art.6 *in fine* del Convenio de 1981, por el sólo hecho de exigir el consentimiento expreso y escrito para ciertos datos sensibles (ideología, religión y creencias) o el mero consentimiento para otros (datos que revelen origen racial, salud y la vida sexual), o establecer una especie de *cautela* [239] de protección para algunos datos sensibles (ideología, religión, creencias, origen racial o vida sexual. Art. 7-4), por la cual se prohíbe crear ficheros "con finalidad exclusiva de almacenar datos", haciendo énfasis solamente a la fase de almacenamiento de datos personales, como si fuera la única etapa de alto riesgo o vulnerabilidad en un proceso informatizado de datos.

Más aún, como sostiene el profesor *Morales Prats* [240], la LORTAD no ofrece un régimen de garantías suficientemente firme para la informatización de los referidos datos. Así, para los datos relativos a la ideología se limita a exigir el consentimiento del titular de los datos por escrito; con respecto a los datos relativos al origen racial o a la vida sexual, el art. 7 LORTAD se limita a exigir que concurran razones de "interés general" reconocidas por una ley, que justifiquen la informatización, lo cual contraria el art. 6 del Convenio de 1981, pues no se encuentran razones que justifiquen la informatización de los datos personales sobre la vida sexual o el origen racial del individuo. La informatización de estos datos sólo puede albergar un interés
legítimo de tipo estadístico y, para tal menester, no es precisa la identificación del titular de los datos; por tanto, la LORTAD debía haber exigido como garantía la previa disociación de éstos, al objeto de que el titular no pudiera ser identificado.

---

(239) MORALES PRATS, F. Ob. cit., pág.309 y ss.
(240) Ibídem, pág. 309 y ss.

B. Excepciones al derecho de acceso, rectificación y cancelación en los Ficheros de Titularidad Pública, sin el consentimiento del titular de los datos (art.21, en relación con los arts. 7-2 y 7-3).

El artículo 21 de la LORTAD, es severamente cuestionado en su constitucionalidad por desconocer flagrantemente los derechos estructurales del ejercicio del derecho de *habeas data y el principio del consentimiento* que todo titular de los datos personales ostenta en el tratamiento o proceso informatizado de datos en el Ordenamiento Jurídico Español, sobre la materia. En efecto, el art. 21 LORTAD, inaplica la normativa prevista en el artículo 7.2 y 7.3 LORTAD, para los "datos especialmente protegidos" o *sensibles* durante el tratamiento informatizado (en especial las fases de recolección y comunicación o cesión) en el cual se requiere el consentimiento expreso y escrito para los datos que revelen la ideología, religión y creencias o, el mero consentimiento si los datos se refieren al origen racial, la salud y la vida sexual, cuando se refieren a los denominados ficheros de las Fuerzas y Cuerpos de Seguridad (art. 20-2 a 4), y particularmente, los ficheros con fines policiales.

La inaplicación se fundamenta en la denegación por parte de los responsables de los ficheros del ejercicio de los derechos de acceso, rectificación o la cancelación "en función de los peligros que pudieran derivarse para la defensa del Estado o la Seguridad Pública, la protección de los derechos y libertades de terceros o *las necesidades de las investigaciones* que se estén realizando" (art.21.1).

La norma cuestionada vulnera el Convenio de 1981 y el art. 18.4 CE. En efecto, el art. 9.2. del Convenio, estipula como excepciones *numerus clausus,* al ejercicio de los derechos de habeas data (o de control de los datos de sí mismo), la seguridad pública o del Estado, los derechos y libertades de terceros, y la represión de las infracciones penales, con lo cual quedan por fuera las "necesidades de las investigaciones". Por consiguiente, la lectura constitucional del art. 21.1 LORTAD exige que el precepto, cuando alude a las ´necesidades de la investigación´ como excepción al *´habeas data´* sea interpretado en el sentido del Convenio de Europa de 1981, esto es, como necesidades de la investigación de determinadas y concretas infracciones penales [241]. Todo por incorporar términos indeterminados, difusos o

(241) Ibídem, pág. 309 y ss.

vaporosos que conducen además a una quiebra del principio constitucional de seguridad jurídica (art. 93 CE.), que también se ve vulnerado por la norma recurrida.

C. Tratamiento informatizado de datos sensibles en ficheros de las Fuerzas y Cuerpos de Seguridad, sin consentimiento del titular (art. 20-3).

El artículo 20-3 de la LORTAD, se ha considerado el más polémico de cuantos se han recurrido por inconstitucionalidad ante el Tribunal Constitucional (TC), no sólo porque inaplica legislativamente el ejercicio del derecho de habeas data y el principio del consentimiento que tiene todo titular de los datos personales en un proceso informatizado, sino porque incide abierta, llana y gravemente sobre los *datos sensibles*, altamente protegidos por las legislaciones universales, comunitarias y estatales europeas.

En el art. 20-3 de la LORTAD, se posibilita el tratamiento informatizado de datos personales de la categoría de los sensibles o del *núcleo duro de la privacy*, sin el consentimiento del titular de los mismos cuando "sea absolutamente necesario para los fines de una investigación concreta". Hace énfasis en la etapa inicial del tratamiento, es decir, en la recolección de datos personales sensibles por parte de las Fuerzas y Cuerpos de Seguridad del Estado. Se estima que con este proceder, la LORTAD, vulnera los arts. 18.4 y 16.2 de la CE, así como el Convenio Europeo de 1981, que proscribe todo tratamiento informatizado de datos personales de la categoría de los sensibles, " a menos que el derecho interno provea garantías apropiadas" (art. 6 *in fine*) , para cualquier fin, incluido el policial.

Sin embargo, sobre el particular hay discrepancia en la doctrina ibérica, pues se considera, por unos **[242]**, que es factible el tratamiento informatizado de datos y obviamente su recogida, así sean datos sensibles de la persona, "ya que de otro modo sería prácticamente imposible el esclarecimiento de la mayoría de los casos investigados". Otros **[243]**, consideran que es inconstitucional el tratamiento informatizado de datos personales sensibles, más aún sin el consentimiento del titular, pudiera --sostienen-- justificarse dicho tratamiento de datos personales generales sin requisitos, "ya que los fines de una investigación concreta pueden entenderse incluidos

(242) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, A. Ob. ut supra cit., pág. 7.
(243) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 28

en las excepciones del art. 9 del Convenio Europeo de 1981". No obstante, el Convenio como sostuvimos contiene unas excepciones *numerus clausus* entre las que no están las "investigaciones concretas" como causal de aquellas. En cambio, sí se menciona las "investigaciones científicas" o los datos personales "con fines estadísticos", siempre "que no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas" (art.9-3 Convenio) inmersas en las denominadas "restricciones" al ejercicio del derecho de información y el habeas data que tiene el titular de los datos en un proceso informatizado, pero no pueden interpretarse como investigaciones concretas (Preguntamos: ¿sobre qué, para qué y por qué?, pues los términos encierran una indeterminación conceptual y temática y por lo ambigua conduce a arbitrariedad de quie- nes las apliquen) ni tampoco son excepciones al ejercicio de derechos sino restricciones.

Unos y otros, concluyen al final, aún matizando sus considerandos que el art. 20-3, es inconstitucional porque vulnera el art. 18.4 en la medida que no hay justificación objetiva de que sea necesario la recogida de esos datos para la protección de la seguridad pública ni ningún otro bien jurídico constitucionalmente protegidos.

Más aún, la CE, no obliga a nadie a declarar sobre su ideología, religión o creencias (art.16-1); vale decir, que la persona no esta obligado a dar su consentimiento, ni nadie esta obligado a exigírselo sobre esta clase de datos personales considerados sensibles, tanto para revelarlos y con mucha mayor razón cuando se trate de someterlos a un proceso informatizado o no de datos.

D. Comunicación (por cesión) interadministrativa de datos personales, sin consentimiento del titular (art. 19.1., en relación con el art. 6.2 y 11-2, e).

El art. 19.1 de la LORTAD, es inconstitucional, según el profesor *Morales Prats* [244], por vulnerar la garantía de reserva de la ley orgánica en el desarrollo de los derechos y garantías que derivan de la libertad informática (art. 18.4. CE). Igualmente, se inaplica legislativamente el principio del consentimiento del titular de los datos en las fases inicial o de recolección, comunicación e incluso de "uso" de

datos personales cuando se trata de ficheros de titularidad pública previstos en la LORTAD (arts. 18 y ss.), aún rebasando más las excepciones al consentimiento previstas en los arts. 6.2 y 11.2-e, de la misma LORTAD, excepciones que corren igual suerte de inconstitucionalidad que el art. 19.1. La rebaja de las garantías mínimas de los derechos y libertades fundamentales de la persona y del principio del consentimiento como una de aquéllas y previstas del Convenio Europeo de 1981, se ven reducidas a su más mínima expresión, pues lo deja inoperante; vale decir, inaplicable al tratamiento y "*uso*" de los ficheros de titularidad pública. La inaplicabilidad o inoperancia del consentimiento del titular conlleva a un cierto determinismo de aquél por parte de las Administraciones Públicas, a tal punto que lo hace nugatorio y de paso desnaturaliza también el "principio de la afectación" [245] de los datos previstos en el art. 5 del Convenio Europeo de 1981 y art. 4.2. de la LORTAD.

El recurrido artículo deniega la comunicación (por cesión) de datos personales interadministrativas de los datos personales recogidos o tratados por procesos informáticos por las Administraciones Públicas, "salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso".

El principio del consentimiento, considerado nuclear en el proceso informatizado de datos español, contiene unas excepciones cuando se trata de ficheros de titularidad pública (art.6-2 LORTAD). En efecto, no se requerirá consentimiento, "cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias". Concordantemente el art. 11.2-e, no precisa el consentimiento del titular de los datos en la comunicación interadministrativa de los mismos en relación con los eventos del art. 19 LORTAD. Se deduce claramente que las excepciones están dirigidas exclusivamente a las fases inicial (recolección) y comunicación (por cesión) del tratamiento informatizado, pero además que la cesión estuviese prevista en la creación del fichero de titularidad pública respectivo y por disposición general publicada en el BOE o Diario Oficial correspondiente (art. 18-1 LORTAD) o por disposición posterior *que regule su uso* (art.19-1 in fine). Quizá por esto último, se diga que la inconstitucionalidad se acentúa más, porque la Administración tiene una carta blanca para poder entrecruzarse datos sin ninguna

(244) MORALES PRATS, F. Ob. cit., pág.309 y ss

(245) "Pero, además, otra garantía básica de la libertad informática (art. 18.4), cual es la expresada en el art. 5 del Convenio del Consejo de Europa y en el art. 4.2.de la LORTAD, alusiva al principio de afectación (ligado al consentimiento del titular) del tratamiento automatizado de los datos personales a determinada finalidad, queda seriamente comprometida por el art. 19.1 LORTAD; este precepto posibilita la alteración de la finalidad del tratamiento de los datos (trámite cesión de los mismos), mediante normas de cobertura de carácter meramente reglamentario (cfr. Arts. 18.1 y 19.1 LORTAD)". Cfr. MORALES PRATS, F. Ob. cit., pág.309 y ss

dificultad, obteniendo aquellos a los que, en principio y debido a sus competencias, no les permitía acceder. No se trata de una delegación que el legislador hace en favor de la Administración, sino que supone una auténtica deslegalización que no se ajusta a límite o control alguno y, por ello, en franca contraposición a la reserva de ley recogida en el art. 53 CE **[246]**.

4.4.4. 3. PRINCIPIO DE RESERVA DE LEY Y SEGURIDAD DE LOS DATOS: DERECHOS Y LIBERTADES FUNDAMENTALES (ARTS. 9-3, EN RELACIÓN CON EL ART. 7 Y EL ART. 17-1)

.

La LORTAD en varios artículos vulnera el principio de reserva de ley previsto en la Constitución Española (art.53-1) y por el cual, sólo por ley, que en todo caso deberá respetar el contenido esencial, podrá regularse el ejercicio de derechos y libertades fundamentales reconocidos en el Capítulo II del Título Primero de la CE, y dentro de los cuales está el derecho a la intimidad, el honor, la imagen, etc. La tutela de dichos derechos y libertades se ejercerá mediante recurso de inconstitucionalidad ante el Tribunal Constitucional (art. 161-1,a). En este aparte nos ocuparemos de dos artículos: el art. 9-3 y el art. 17.1., LORTAD.

A. Principio de seguridad de los datos personales de categoría sensible (ar.9-3).

El art.9-3 LORTAD, establece que mediante Reglamento se establecerán los requisitos y condiciones que deben reunir los ficheros informatizados y las personas que intervengan en el proceso informatizado de datos personales sensibles.

Hemos sostenido, que la legislación universal, y en particular, la Comunitaria Europea, proscribe el sometimiento a proceso informatizado los datos considerados

sensibles, salvo que existan garantías idóneas de protección plena, clara y precisamente establecidas en el ordenamiento jurídico de cada Estado (art. 6 Convenio de 1981). Este principio que también se ha denominado "Principio General de Interdicción", palmariamente se halla vulnerado por el art.9-3, cuando establece que será por "Reglamento" y no por Ley (al menos Ordinaria y de menor entidad que la

---

(246) QUILEZ AGREDA, Ernesto y CEBRIAN DEL MORAL, A. Ob. ut supra cit., pág. 7.

Ley Orgánica) la regulación de requisitos y condiciones que deben reunir los ficheros como las personas que intervienen en el tratamiento informatizado de datos personales de la categoría de los sensibles. Así, se vulnera concomitantemente el art. 53-1, CE, por quebrantar el principio de reserva legal, al dejar en manos del Reglamento, materias o aspectos atinentes a los derechos y libertades fundamentales, que sólo están reservadas exclusiva y excluyentemente a la ley, derechos tales como los previstos en el art. 18.4 CE.

B. Tutela de los derechos fundamentales en el tratamiento informatizado de datos (art. 17-1).

La LORTAD, establece que las actuaciones contrarias a las fases de tratamiento informatizado de datos o de los derechos fundamentales que éstas involucran, pueden ser objeto de reclamación por los titulares de los datos personales ante la Agencia de Protección de Datos, "*en la forma que reglamentariamente se determine*". (art.17-1 *in fine*).

La LORTAD, quebranta el principio de reserva de ley previsto en la CE (art.53-1), en relación con el art. 18.4 y 24.1 CE, cuando en el art. 17.1, remite a una norma de rango inferior (El Reglamento), la Ley de regulación procesal de los Recursos contra actuaciones de los poderes públicos contrarias a ésta [247]. En efecto, con la remisión se involucra aspectos procesales importantes como los eventuales recursos que se desatarían ante la Agencia de Protección de Datos, por desconocimiento o quebrantamiento de derechos y libertades fundamentales previstos en la regulación del tratamiento informatizado de datos de la LORTAD, que siendo objeto de la ley exclusivamente se trasladan al Reglamento.

4.5. LAS DIRECTIVA 95/46/CE Y 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 1995 Y 1997, RESPECTIVAMENTE.

Los recursos de inconstitucionalidad *sub júdice* contra la LORTAD ante el Tribunal Constitucional, como se ha sostenido se ven tocados no sólo por la expedición de normas comunitarias previas, como el Convenio de Estrasburgo de 1981, sino

---

(247) LOPEZ GARRIDO, Diego. *ASPECTOS*... Ob. cit., pág. 25

posteriores a su planteamiento, como la Directiva 95/46/CE, pero previa a la resolución de los recursos. La incidencia jurídica deviene de la transposición normativa [248] que de la Directiva Comunitaria, debe hacer el Estado Español, el 31 de Octubre de 1998, como fecha límite, según la disposición final prevista en el art. 32.1, para que la normativa existente (LORTAD y R.D., que la desarrollan) o las reformas legislativas idóneas (Proyectos que ya cursan en las instancias legislativas [249]) en materia de protección de las personas físicas cuando sometan a tratamiento informatizado sus datos personales se adopten de conformidad con las previsiones de tutela y garantía prevista en la Directiva.

Por ello, haremos un estudio sucinto de los aspectos capitales que plantea la Directiva, y sobre todo, aquellos que hacen referencia a los principios, derechos y garantías de los titulares de los datos personales generales y sensibles y las fases del proceso informatizado de los datos mismos. Así mismo, se hará referencia puntual a una reciente Directiva Comunitaria que incide en la fase de comunicación del proceso informatizado de datos y en los principios y garantías de tutela de los titulares de los datos personales; nos referimos a la Directiva 97/66/CE, *relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas.*

4.5.1. LA DIRECTIVA 95/46/CE, sobre *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

La Directiva 95/46/CE., en materia de *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* contiene una estructura normativa *sui géneris* muy propia de las normas comunitarias

---

(248) Un estudio de los impactos de la transposición normativa en Bélgica con conclusiones comparativas a la transposición de la Directiva de protección de datos en España, puede consultarse, en: DUMORTIER, J. Y ALONSO BLAS, Diana.*LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION DE DATOS EN BELGICA.* En: Actualidad Informática Aranzadi. Ed. Aranzadi, Núm. 20. Julio, Pamplona, 1996, págs. 1-7 y ss.
(249) Un breve comentario al anteproyecto de reforma a la LORTAD, en GUTIERREZ SANCHEZ, Pedro. *ANTEPROYECTO DE LEY ORGANIZA POR LA QUE SE MODIFICA LA LEY ORGANICA 5/1992, DE 29 DE OCTUBRE, DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL (LORTAD).* En: Actualidad Informática Aranzadi. Ed. Aranzadi, Núm. 20. Julio, Pamplona, 1996, págs. 1-4 y ss.

europeas, pertenecientes a las fuentes del llamado Derecho Derivado Comunitario **[250]**

La Directiva esta dividida en dos grandes partes: una, de carácter interpretativo o hermenéutico; y otra, de carácter normativo propiamente dicho, y por ende con efectos jurídicos, dividida en capítulos, secciones y artículos. La primera parte, contiene un amplísimo número de considerandos, 72 en total, los cuales constituyen la exposición de motivos de la norma jurídica; vale decir, la parte de interpretación hermenéutica plasmada por el propio legislador comunitario a fin de desentrañar y justificar el cuerpo del texto normativo. En dichos considerandos está el espíritu y razones de ser de la norma comunitaria, por ello, en el transcurso de esta investigación haremos referencia a aquéllos.

La segunda parte, se estructura así: Capítulo I. *Disposiciones Generales*: Objetivo de la Directiva (art.1), Definiciones (art.2), Ambito de aplicación (art.3), Derecho nacional aplicable (art.4). Capítulo II. *Condiciones generales para la licitud del tratamiento de datos personales:* Secc. I. Principios Relativos a la Calidad de datos (art. 6). Secc. II. Principios Relativos a la Legitimación del Tratamiento de datos (art. 7). Secc. III. Categorías Especiales de tratamiento (arts.8 y 9). Secc. IV. Información del interesado (arts.10 y 11). Sec. V. Derecho de Acceso del interesado a los datos (art.12). Secc. VI. Excepciones y limitaciones (art.13). Secc.VII. Derecho de Oposición del interesado (art. 14 y 15). Secc. VIII. Confidencialidad y Seguridad del Tratamiento (arts. 16 y 17). Sec. IX. Notificación (arts. 18 a 21). Capítulo III. *Recursos Judiciales, Responsabilidad y Sanciones* (arts. 22 a 26). Capítulo IV. *Códigos de Conducta* (art.27). Capítulo VI. *Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de*

datos personales (arts. 28 a 30). Cap. VII. *Medidas de ejecución comunitarias* (art. 31). *Disposiciones Finales* (art.32 a 34).

Los principios de protección a las personas físicas (identificadas o identificables,

---

(250) Este derecho escrito es el creado por los organismos comunitarios (El Parlamento, La Comisión y El Consejo, especialmente). Comprende en primer término, los actos jurídicos expresamente previstos en los Tratados de creación de la CE (hoy UE, Unión Europea); actos que contienen reglamentaciones obligatorias para los Estados Miembros. Estos son: los Reglamentos, LAS DIRECTIVAS, y las Decisiones dirigidas a particulares y al Estado Respectivo; así como las Recomendaciones o razones que emanan del Tratado de la CECA, y los Acuerdos Internacionales que conciernen a la Comunidad Europea. Mis trabajos:*LAS FUENTES DEL DERECHO COMUNITARIO EUROPEO.* En: Revista FORO UNIVERSITARIO. Ed. UNED, Univ. de Nariño, Núm. 15, Pasto, 1988, pág.65-75; y, *LOS DENOMINADOS RECURSOS ANTE LOS TRIBUNALES DE JUSTICIA DE LA C.E Y ANDINO.* Ed. UNED, Universidad de Nariño, Pasto (Colombia), 1995, pág. 11 y ss.

no anónimas **[251]**) en el tratamiento informatizado o manual (aunque sólo extensible a los denominados *ficheros* no a las *carpetas* de datos) **[252]** de datos personales, previstos en la Directiva, tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos. Estas obligaciones, se refieren en particular, a la calidad de datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento. De otra parte, estos principios hacen referencia a los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, tales como, el de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias **[253]**.

4.5.1.1. GLOSARIO DE TERMINOS IUSINFORMATICOS: DEFINICIONES TECNICO-JURIDICAS.

En tal virtud, y antes de abordar el análisis referencial de los principios de protección de los titulares de los datos personales, hagamos referencia a las definiciones de los conceptos aplicables al tratamiento informatizado de datos, pues éstas constituyen el glosario indispensable para el entendimiento jurídico-técnico de la Directiva, y lo que es más importe aún, conducen a una mejor interpretación hermenéutica de los conceptos básicos para el tratamiento de datos personales, que tienen por objeto garantizar el respecto a los derechos y libertades fundamentales, en

(251) En similar sentido, los considerandos 25, 26, 68 y 72 de la Directiva.

(252) Según el considerando 27, "La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su *tratamiento manual*; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los *ficheros*, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva".

(253) Para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. Por tanto, los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado. Los códigos de conducta con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado (Considerando 26).

particular en derecho a la intimidad, reconocido en el Convenio Europeo para la protección de Derechos Humanos y de las Libertades Fundamentales (art. 8), así como en los principios generales del Derecho Comunitario y el Convenio de 28 de Enero 1981, que protege el conjunto de derechos y libertades fundamentales (incluido la intimidad) en el curso de un tratamiento informatizado, precisado y ampliado por la Directiva en éstos menesteres (C. 10 y 11).

En efecto, *Datos personales*, se considera *toda información sobre una persona física identificada o identificable (el interesado); se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social* (art.2-c). Esta definición, incorpora elementos de forma y de fondo empleados en la identificación plena de una persona humana, a efectos de evitar al máximo el error, la indeterminación o la confusión del titular de unos datos personales que le conciernen o le puedan concernir si se reputa identificable directa o indirectamente, o lo que es lo mismo, la persona interesada. Esta definición cualificada de persona física a la que le corresponde una información de carácter personal, elimina las dificultades generadas en torno identificabilidad, no sólo por medios documentales tradicionales (DIN o DNI, etc), sino por elementos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; vale decir, por las caracteres relevantes de la identidad heredo-biológica de la persona, su hábitat social y cultural y hasta su nivel socio-económico. Se crea así

una especie de derecho a la identificación como garantía de los derechos fundamentales asignados a una persona humana, cuando sean sometidos a tratamiento informatizado o manual datos personales.

Los distintos elementos característicos definidores de la identidad de una persona permiten además, a los Estados Miembros de la UE, estructurar en su normas reguladoras de la protección de derechos y libertades fundamentales y del proceso informatizado de datos personales, según se sostiene en el C. 27, de la Directiva, que se regule, entre otros aspectos importantes, el ejercicio del derecho de *habeas data*, en particular, el derecho acceso a dicho conjunto de datos; así mismo que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la Directiva 95/46/CE.

El *Tratamiento de datos personales,* se considera a *cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicables a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción* (art.2-b). Esta definición cualificada, a diferencia de la actividad rehusada por el grupo de expertos del Convenio de 1981 para hacerlo, conlleva unos elementos técnicos, jurídicos y acciones informáticas con los denominados archivos o registros informáticos (o *file*), incorporados o por incorporar en una base de datos (*database*) o ficheros informatizados (*fichiers*), que en su conjunto conforman el proceso o "procedimiento automatizado" de datos personales.

En efecto, son etapas o fases de un procedimiento informatizado de datos, la recolección, almacenamiento, registro, conservación y comunicación (por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión. Aspectos técnicos idóneos que posibilitan el nuevo fenómeno tecnológico de la comunicación y la información : TIC). Las acciones de consulta, extracción, bloqueo, supresión o destrucción, modificación incorporadas en la definición de tratamiento de datos personales, que bien pueden hacerse con medios informáticos, electrónicos o telemáticos sobre archivos o registros (o

simplemente datos) contenidos en ficheros informatizados o bien con medios mecánicos o manuales en ficheros de idéntica índole, engloban el concepto genérico de "tratamiento" previsto en la Directiva en forma multicomprensiva.

El *Fichero de datos personales,* se entiende *todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado o repartido en forma funcional o geográfica* (art. 2-c).

Cabe resaltar de la definición que los "criterios determinados", son aquellos establecidos en la correspondiente normativa estatal sobre el tratamiento informatizado de datos personales, el ámbito de aplicación de dicha normativa, y sobre todo, los elementos característicos de la persona identificable que antes puntualizábamos, pues ellos indicarán la menor o mayor cobertura de protección de los derechos y libertades fundamentales de la persona. Una normativa miope en éstas lides sería la que estipula la identificabilidad de la persona por el sólo criterio documental v.gr. El D.N.I. o DIN.

En igual forma, la definición *fichero* amplía los criterios de ámbito de aplicación de la normativa a los aspectos de distribución de competencias por servicios (centralizado o descentralizado), territorial (o geográfico) y funcional, teniendo en cuenta la estructura estatal de los Estados Miembros de la UE (Estados Unitarios, Federales o Comunitarios, como el Español).

El *Responsable del tratamiento*, es quizá con el de "tratamiento de datos personales" dos de los conceptos más elaborados en la Directiva, por su íntima correspondencia temática, los efectos jurídicos y materiales y las implicaciones en los ámbitos de tutela, garantía, régimen de responsabilidades y sanciones y derechos y deberes de los sujetos intervinientes en el proceso o procedimiento informatizado (el titular de datos, "encargado del tratamiento" **[254]**, el responsable del fichero, "el tercero"**[255]** y "el destinatario" **[256]**).

Así, se considera *Responsable del Tratamiento* (institución jurídica más amplio y precisa que la de "responsable del fichero", utilizada por la LORTAD **[257]**), es *la* _____

(254) El "encargado del tratamiento", es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento (art. 2-e)

(255) El "Tercero", es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distintodel interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento (art. 2-f).

(256) El "*Destinatario*", es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios (art. 2-g).

(257) En la Doctrina Ibérica, se ha sostenido la deficiente definición de la figura del responsable del fichero realizado por la LORTAD; entre otras, por las siguientes razones: a) la determinación de este sujeto se realiza conforme a *varios criterios,* sin determinar cuál es de aplicación en cada caso, por lo que se plantea el problema de si el titular del fichero puede optar entre uno u otro criterio a la hora de señalar quién es dicho responsable --con la consiguiente posibilidad de manipulación y utilización estratégica de las distintas posibilidades que se contienen en la definición legal del responsable del fichero, para eludir la propia potestad sancionadora con el correlativo compromiso de la funcionalidad general del sistema--; b) la particular y no menos deficiente descripción del responsable del fichero en el ámbito público que determina la imposibilidad de aplicar los criterios legalmente previstos a determinados ficheros que, por el contrario, sí se encuentran sometidos al ámbito de aplicación de la ley --como es el caso de los órganos constitucionales-- que por su especial estructura jurídica no tienen fácil acomodo en ninguna de las categorías contempladas en la definición legal; y, c) la falta de distinción entre el responsable del fichero y el encargado del tratamiento, sujeto que, sin perjuicio de realizar actividades con indudable incidencia en el campo que analizamos --que determinan su sumisión específica al deber de guardar secreto (art.10 LORTAD)-- no se encuentre sujeto a responsabilidad alguna. Vid. DE LA SERNA BILBAO, María Nieves. *LA AGENCIA DE PROTECCION DE DATOS ESPAÑOLA: CON ESPECIAL REFERENCIA A SU CARACTERISTICA DE INDEPENDENCIA*. En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 22 de Enero, Pamplona, 1997, pág. 3

persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios de tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario (art. 2-d).

A través de la naturaleza jurídica y funciones genéricas y específicas del responsable del fichero en el transcurso del procedimiento informatizado de datos, se logra caracterizarlo, tal y como lo delinearon los legisladores comunitarios. En efecto, aquélla y algunas de éstas, son:

a) *Naturaleza jurídica*: La Directiva deja al ámbito legislativo de los Estados la determinación de sí, el responsable del tratamiento debe tener una misión de interés público o inherente al ejercicio del poder público, o si debe ser una administración pública u otra persona de derecho público o privado (considerando 31). La amplitud de la naturaleza jurídica del responsable del tratamiento identifica el amplio o reducido abanico de funciones, derechos, obligaciones y niveles de responsabilidades que debe asumir aquél. v.gr. En la transmisión de un mensaje con datos, a través de un servicio de telecomunicaciones o de correo electrónico cuyo

único objetivo sea transmitir mensajes de este tipo, será considerado responsable del tratamiento de datos, aquélla persona de quien procede el mensaje y no la que ofrece el servicio de transmisión [258].

b) *Ambito de Aplicación*. Serán aplicables los principios de protección de datos previstos en la Directiva, a todos los tratamientos de datos (total o parcialmente informatizados, así como a los informatizados siempre que puedan ser incluidos en un fichero) en los cuales las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho Comunitario, salvo que expresamente estén excluidas [259].

---

(258) Sin embargo, pueden reputarse, llegado el caso, en responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio) (Considerando 47, *in fine*).

(259) Se excluyen: a) El ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI, del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de fatos que tenga por objeto las seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del mismo Estado en materia Penal; y, b) Los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. v.gr. La correspondencia y llevanza de un repertorio de direcciones (Art. 3-2., conc. con el considerando 12).

c) *Identificabilidad de una persona*. A efecto de aplicar el sistema de protección arbitrado para las personas, en particular el derecho de información que a ésta le asiste como persona identificada o identificable, el responsable del fichero deberá tomar para determinar la identificabilidad de la persona, el "conjunto de los medios que puedan ser razonablemente utilizados" por éste o por "cualquier otra persona", para identificarla (C. 26).

d) Limitación de las funciones, por excepciones *numerus clausus*. Los Estados en sus legislaciones internas, pueden imponer restricciones a determinadas obligaciones del responsable del tratamiento, cuando sean necesarias para salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas (C. 43);

e) *Funciones por encargo*. Para evitar que una persona quede excluida de la protección garantizada por la Directiva, será necesario que los Estados prevean que cualquier persona que efectúe tratamientos de datos, por cuenta del responsable

("encargado del tratamiento") actúe bajo la autoridad y responsabilidad del responsable del tratamiento establecido en cada legislación estatal (C. 18).

El responsable o encargado del tratamiento no serán dispensados de las demás obligaciones que les conciernen conforme a la Directiva o la normativa estatal correspondiente, diferentes a los de notificación a los sujetos involucrados en el tratamiento informatizado de datos, en aquellos casos, por ejemplo, que tengan como fin evitar trámites administrativos improcedentes o innecesarios en torno a la exención o simplificación de la notificación para los tratamientos de datos, siempre que no atenten contra los derechos y libertades de los interesados (C. 49 y 51).

f) *Recurribilidad de los Actos del Responsable del tratamiento*. A fin de que se respeten los derechos de los interesados por parte de los responsables de los ficheros, los Estados en sus legislaciones arbitrarán un "*recurso judicial*". Los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor (C. 55);

g) *Funciones de garante en la comunicación de datos*. Podrán adoptarse "medidas particulares" para paliar la insuficiencia del nivel de protección de un tercer país, siempre que el responsable del fichero ofrezca "garantías adecuadas" en la comunicación de datos personales entre Estados ("Flujos internacionales"), previos la existencia de instrumentos legales y procedimientos de negociación entre la Comunidad y los países terceros, sobre la materia (C. 20 y 59).

4.5.1.2. PRINCIPIOS FUNDAMENTALES APLICADOS A LAS FASES DEL PROCEDIMIENTO INFORMATIZADO DE DATOS PERSONALES.

4.5.1.2.1. NOTAS PRELIMINARES AL SISTEMA DE PRINCIPIOS.

El sistema de principios fundamentales en el procedimiento informatizado de datos personales con vista a la Directiva 95/46/CE, contiene unas directrices de interpretación hermenéutica previstas en los considerandos (C), a saber:

a) Las legislaciones estatales que regulan el tratamiento informatizado de datos personales, tienen por objeto garantizar el respeto de los derechos y libertades fundamentales (incluido el derecho a la intimidad) y los principios generales del Derecho Comunitario. En consecuencia, la aproximación de dichas legislaciones a las directrices de la Directiva, no deben conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la UE (C.10).

b) Los principios de protección de los derechos y libertades de las personas, precisan y amplían los del Convenio Europeo de 1981 (C.11).

c) Los principios se aplican a todos los tratamientos (total o parcialmente informatizado, incluso los manuales cuando los datos están contenidos o destinados a ser incluidos en un fichero) de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito del Derecho Comunitario. La exclusión es taxativa, vale decir, *numerus clausus* --art. 3-2-- (C.12)

d) Los principios de protección se aplicarán en forma restringida en los tratamientos de sonido y de la imagen **[260]** con fines periodísticos o de expresión literaria o artística (C.17) **[261]**. Es decir, que los principios de protección de las personas en un procedimiento informatizado de datos se aplicarán en la medida que resulten necesarios para la conciliación del derecho a la intimidad con las normas que rigen la libertad de expresión.

e) Los principios tienen su expresión en dos ámbitos correlacionados, a saber: uno, las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos (v.gr. calidad de datos, seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento); y otro, los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su

rectificación o incluso de oponerse a su trata miento en determinadas circunstancias (C.25). Huelga decir, los derechos estructurales del ejercicio del derecho de *habeas data* y el derecho de oposición al tratamiento informatizado de datos por parte de los titulares, previstos en los arts. 10 a 12 y 14 de la Directiva, respectivamente. Derechos base y fundamento de la visión iusinformática de los derechos y libertades fundamentales, como hemos visto.

---

(260) Como lo confirman Dumortier y Alonso Blas, "Si bien la Ley Orgánica no aludía en concreto a dichos conceptos, sí se aludía a los mismos en el art. 1-4 del Reglamento de la Agencia (D.R.1332/1994, de 20 de Junio) -- información fotográfica, acústica o de cualquier otro tipo). En todo caso, en la Directiva se amplía más el dato personal de imagen al incluir no sólo la captada por aparato fotográfico, sino también por videocámaras y, en definitiva, por lo que puede definirse como sector audiovisual (agregaríamos con medios informáticos, electrónicos o telemáticos que manejan el dato personal de imagen, tal como precisaremos en la parte III y IV de esta investigación). No cabe duda que la utilización de imagen y sonido ha experimentado un gran aumento : controles de acceso a edificios, fichero de policía, utilización de la voz en el automóvil o de la imagen en controles de acceso en autopistas, en detección de infracciones de tránsito, en los servicios y comercio mediante los terminales de información, en el mundo del trabajo y de las relaciones profesionales, en el ámbito del hogar o en el terreno de la salud. El reconocimiento de la voz y el sonido como datos personales efectuado por la Directiva va a potenciar la protección de los mismos en aras de la salvaguarda de la intimidad personal (o mejor al conjunto de derechos y libertades fundamentales previstos en la CE, en el ámbito español)..." DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION DE DATOS EN BELGICA.* En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 20 de Julio, Pamplona, 1997, pág. 5

(261) Conforme al art.9 de la Directiva, los Estados aplicarán "*exenciones* y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad expresión", cuando se trate de la aplicación de los Capítulos (IV), "Transferencia de datos personales a países terceros" y Capítulo VI, "Autoridades de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales".

f) Los principios de protección se aplican a cualquier información relativa a una persona identificada o identificable (art. 2-a Directiva). Por contra, no se aplicarán a los datos hechos anónimos de tal manera que ya no sea posible identificar al interesado (C.26); y,

g) El Sistema de principios de protección de los derechos y libertades de las personas, según el C.68, no es un sistema acabado, puesto que los Estados podrán completar y precisarlo, "sobre todo en determinados sectores, mediante normas específicas conforme" a los principios previstos en la Directiva.

Ahora bien, los principios de protección de los titulares de los datos previstos en la Directiva, aplicados a las diferentes fases del proceso informatizado de datos, que a la vez las estructuran y dan contenido, las podemos clasificar y

enunciarlos así: a) Fase de recolección de los datos; b) Fases de almacenamiento, registro y conservación de los datos; y b) Fase de Comunicación de los datos.

Sin embargo, como principio directriz de todo el procedimiento total o parcialmente informatizado o manual, siempre que los datos vayan a constituir parte de un fichero, la Directiva a erigido como actividad ineludible y de resorte del responsable del tratamiento, o en su caso, su representante, el que denominaremos *principio previo de notificación a la autoridad de control*, prevista en el art.28 de la Directiva. Esta autoridad de control, como autoridad pública, encargada de vigilar la aplicación en cada territorio estatal de las disposiciones de la Directiva, que tiene como objetivo primordial, la protección de los derechos y libertades fundamentales de las personas físicas en lo que se refiere al tratamiento de datos personales, con funciones atribuidas con total independencia y con poderes de investigación, poderes efectivos de intervención y con capacidad procesal en caso de infracciones a la Directiva. Las decisiones de esta autoridad que causen lesión a los derechos serán objeto de recurso jurisdiccional (art. 28 Directiva).

Con fundamento en este principio fundamental previo al tratamiento de datos personales, el responsable del tratamiento o, en su caso, su representante efectuarán una notificación a la autoridad de control, siempre que dicho tratamiento vaya destinado a la consecución de un fin o de varios fines conexos.

La notificación, como uno de los *mecanismos de control* previo que deben adoptar los sujetos involucrados en iniciar un tratamiento de datos personales para eludir cualquier suposición de riesgo para los derechos y libertades de las personas deberán velar porque se cumpla a cabalidad “antes del comienzo del tratamiento” (art.20. Ibídem).

La notificación contiene como mínimo la siguiente información: a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; b) el o los objetivos del tratamiento; c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento; d) los destinatarios o categorías a los que se pueden comunicar los datos; e) las transferencias de datos previstas a países terceros; f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas con

motivo de la seguridad del tratamiento (art.17 Directiva) resultan adecuadas para garantizarlo.

4.5.1.2.2. FASE INICIAL O DE RECOLECCION DE DATOS.

En la *Fase inicial o de Recolección de datos,* se aplicarán algunos de aquellos principios relacionados en el grupo de principios relativos a la "calidad de los datos" (art. 6), el grupo de los principios relativos a la "legitimación del tratamiento de los datos (art.7) y en las "Categorías especiales de tratamiento" de los datos (art.8) de la Directiva. Valga decir, que varios de los subsiguientes principios no sólo se aplican a la fase de recolección de datos, sino a todo el procedimiento informatizado, tal como lo anotaremos puntualmente al comentar cada uno de estos. En efecto, estos son:

a) *El principio de compatibilidad de la recolección de los datos con las finalidades del tratamiento*. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías adecuadas (art. 6-b).

b) *Principio de proporcionalidad (pertinencia, adecuación y no excesibilidad) de los fines.* Los datos que se recaben (o recojan) deben guardar la proporcionalidad de esta actividad con los fines de tratamiento posteriores, es decir, que deben ser adecuados, pertinentes y no excesivos en relación con dichos fines (art. 6-c).

c) Principio de lealtad y licitud. Este principio, también conocido como de legalidad (que no legitimidad, como se suele confundir [262]), es aplicable a todo el tratamiento informatizado de datos personales, y obviamente a la etapa inicial del proceso conocida como de recolección de datos. En tal virtud, toda recolección de datos personales deberá hacerse de conformidad con el ordenamiento jurídico vigente sobre la materia en cada Estado, siguiendo para ello las directrices previstas en la Directiva. Es decir, que el tratamiento sea lícito. Si una persona sufre un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible

con las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE., aquella tendrá derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. Según el art. 23-2 de la Directiva, el responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Que el tratamiento de datos sea leal, supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención (C.38).

d) *Principio de veracidad y exactitud de los datos*. Los datos personales que se recaben deben responder a la verdad y exactitud vertida por los titulares de la misma, tanto si ha sido recolectada del propio interesado como si no fuesen recabados de éste.

Los sujetos involucrados en el tratamiento de datos, principalmente el responsable o encargado del tratamiento, deberán tomar las medidas razonables para que los datos no sean inexactos o incompletos; y llegado el caso, si lo fuesen y contrarían además el principio de la proporcionalidad de la recolección con los fines, puedan posteriormente ser suprimidos o rectificados, tras el ejercicio del *habeas data*

---

(262) En este sentido, se mencionan los principios relativos a "*la legitimidad del tratamiento de datos*" (art.7 Directiva), como una explicación del principio de lealtad y licitud de los datos (art.6-1 Ibídem). BETES DE TORO, Alfredo. *El DERECHO DE INFORMACION Y LOS PRINCIPIOS LEGITIMADORES DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARACTER PERSONAL EN LA DIRECTIVA 95/46/CE, DE 24 DE OCTUBRE DE 1995*.En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 25 de Octubre, Pamplona, 1997, pág. *7*

(acceso, rectificación, actualización y cancelación) por parte del interesado.

e) *Principio de legitimidad de la recolección de datos.* Este principio es de capital importancia en la protección de derechos y libertades fundamentales, y en particular de la intimidad, cuando los datos personales sean sometidos a procedimiento informático.

Además, éste principio engloba otros que se consideran estructurales o continentes de éste, tales como el principio del consentimiento (columna vertebral de la LORTAD), el principio de finalidad del tratamiento de datos y el de prevalencia de ciertos intereses en el tratamiento de datos, tales como, los intereses vitales para el interesado, el interés público para los poderes públicos o los intereses legítimo para el responsable del tratamiento. Quizá por ello, el concepto jurídico de legitimidad rebasa al de la simple legalidad, pues aquélla es más amplia y de aplicación *erga omnes* a los sujetos involucrados en el tratamiento de datos personales, pues está fundada en criterios de la legalidad, de valores o de intereses públicos o particulares, y no simplemente normativos como es el caso de la legalidad.

Este principio de la legitimidad del tratamiento **[263]** se aplica a todo el tratamiento de los datos, y por obvias razones, a la primera fase inicial o de recogida de datos. En tal virtud, siendo la legitimidad más amplia y genérica que la legalidad, pero ambas dirigidas a la protección de derechos y libertades fundamentales , la Directiva 95/46/CE, establece unas líneas directrices que legitiman el tratamiento de datos. Estos son:

1. El *principio del consentimiento* que requiere para todo el tratamiento de datos, y en particular, para la etapa inicial de recolección de la información. El consenti-

---

(263) Se ha considerado de tal importancia este principio (aunque se los autores hablan de principio de legalidad), que comentan que el legislador belga, al abordar el tema de la transposición de la normativa Comunitaria (Directiva 95/46/CE), "tiene la intención de incluir literalmente el texto del artículo 7... en el nuevo proyecto de ley de protección de datos. El motivo de esta transposición literal se funda en el concepto de Directiva como instrumento de Derecho Comunitario que autoriza a los Estados Miembros para decidir la forma y medios para su cumplimiento, pero les obliga en forma estricta en cuanto a su contenido". Al fin y al cabo, como antes sostuvimos la Directiva es una norma jurídica comunitaria de carácter obligatorio para los Estados Miembros, pues pertenece a las fuentes del llamado "Derecho Derivado Comunitario" Cfr. DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION*... Ob. cit., pág. 8.

miento del interesado o titular de los datos deberá ser en forma inequívoca y explícita, salvo las excepciones *numerus clausus* previstas en la Directiva cuando se trata de "categorías especiales de datos" (art. 8-1 a 8-3, Directiva) **[264]**.

2. *El principio de finalidad de los datos*. Principio que se estructura en las siguientes eventualidades: a) Cuando el tratamiento es necesario para la ejecución de un contrato en el que sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; y, b) Cuando el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.

3. *El principio de prevalencia de ciertos intereses públicos y particulares*. Este principio se presenta en los siguientes eventos: a) Cuando sea necesario para proteger un *interés vital* del interesado; b) Cuando sea necesario para el cumplimiento de una misión de *interés público* o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen datos; y, c) Cuando sea necesario para la satisfacción del *interés legítimo* perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que prevalezca el interés o los derechos y libertades fundamentales del interesado que requie- ran protección, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de datos personales.

f) *El principio de interdicción de tratamiento de datos personales pertenecientes a las "Categorías Especiales*". La regla general, es la prohibición del tratamiento respecto de los datos personales inmersos en la categoría de especiales (que incluye a los denominados datos "sensibles" o hipersensibles, comentados por la doctrina ibérica [265])que revelen el origen racial o étnico, las opiniones políticas, las convicciones

---

(264) En dicha categoría se incluyen los denominados por la doctrina anglosajona como los datos del "núcleo duro de la privacy" (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad) -- Art.8-1--; En cuanto a las excepciones taxativas, giran en torno al concepto del consentimiento explícito e inequívoco del interesado o titular de los datos personales.

(265) Veáse, p.e., en la obras citadas ut supra, a CASTELLES ARTECHE, SOUVIRON, FAIREN GUILLEN, ORTI VALLEJO, MORALES PRATS, BAJO FERNANDEZ, en las visiones de aquellos datos sensibles, hipersensible y aún con plus especial de hipersensibilidad en materia constitucional, administrativa, civil y penal, respectivamente. En la parte III y IV, de la investigación ahondaremos más sobre el tema.

religiosas o filosóficas, pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. La interdicción al tratamiento se funda en la naturaleza de los datos personales, los cuales pueden atentar contra los derechos y libertades fundamentales, y en especial, contra la intimidad, las cuales *a priori* no deber ser objeto de tratamiento alguno (informatizado o manual) de datos .

La excepción a la regla la constituye el consentimiento inequívoco y explícito del interesado o titular de los datos personales. Las excepciones taxativas [266] o, *lista cerrada de datos* [267] exceptuados, pero al fin y al cabo lista considerablemente amplia y posibilitadora de acrecentamiento por "motivos de interés público importantes" (art.8-4), o por "disposiciones nacionales que prevean garantías apropiadas y específicas" en materia de datos relativos a infracciones, condenas penales o medidas de seguridad (art.8-5 *ab initio*) en la Directiva y fundada en criterios de legitimidad (derechos, valores, intereses públicos y privados) y no de simple legalidad. Estas causales de excepciones maleables en cada Estado Miembro, como medida de control de la UE, deberán ser notificadas a la Comisión, si se llegaren a adoptar en las legislaciones internas respectivas (art.8-6).

---

(266) Las excepciones son: a) Cuando el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho Laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas; b) Cuando el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; c) Cuando el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por un fundación, una asociación, o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados; d) Cuando el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) Cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por una profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto (art. 8-3); f) Cuando el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado Miembro basándose en las disposiciones nacionales que prevean garantías apropiadas y específica. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos (art. 8-5 *ab initio*); g) Cuando el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos (art. 8-5 *in fine*); h) El "número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento", si los Estados UE, así lo consideran en condiciones especiales (art.8-7). Texto completo en la dirección electrónica: WWW. CC.CEC (DATABASE CELEX).

(267) DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION DE LA DIRECTIVA*... Ob.cit., pág. 9

Quizá tal vez, por esa amplitud y acrecentamiento de excepciones, se pueda pensar metafóricamente que la regla prohibitiva al tratamiento de datos, constituye el prisma del cual se refleja un arcoiris de excepciones, que por serlas siguen teniendo como referente a la regla, pero con cierto temor fundado de desvirtuarla. Muy a pesar, se piensa por un sector de la doctrina hispana [268], que aún teniendo la lista de excepciones un "carácter limitativo", pero ampliable por cada Estado

Miembro de la Comunidad --en nuestro sentir demasiado amplísima, aún considerando los fundamentos de las excepciones basadas en la heterogeneidad de los Estados Miembros de la Comunidad que propenden al ser UE., por una homogeneidad, al menos legisla-tiva-- resulte un punto poco claro que, basándose en declaraciones incluidas en el acta de la sesión del Consejo en que se aprobó la posición común de la Directiva, se afirme en buena lógica que los Estados miembros podrán precisar o concretar las categorías de datos calificados como sensibles, teniendo en cuenta las características jurídicas y sociológicas de cada país. La Dirección General XV de la Comisión Europea ha confirmado en todo caso el carácter limitativo de esta lista, afirmando que las mencionadas declaraciones incluidas en las actas del Consejo *no tienen valor jurídico alguno* .

Pues bien, las excepciones previstas en los arts. 8 y 9 de la Directiva deben constar igualmente en forma explícita y se justifican sólo por "necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales" (C.33).

Igualmente la Directiva autoriza a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la

---

(268) Ibídem, pág. 9 y 11. Cita para corroborar su argumento a HEREDERO HIGUERAS, M., *LA LEY ORGANICA 5/1992, DE REGULACION DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARACTER PERSONAL: COMENTARIO Y TEXTOS.* Ed. Tecnos, 1996, pág. 99.

rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas (C.34).

Así mismo, se justificará el tratamiento de datos personales, en los siguientes casos: a) por parte de las autoridades públicas con fines, establecidos en el Derecho Constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realice por motivos importantes de interés público (C.35); b) en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados Miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas (C.36); y c) para el tratamiento de datos personales con *fines periodísticos o de expresión artística o literaria*, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias *a posteriori* como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales (art. 9 y C.37).

g) El *Principio de la información del interesado o titular de los datos*. Capital importancia adquiere el derecho a la información en el proceso informatizado de datos, pues es aplicable a todo el tratamiento, y por consiguiente, a la fase de recolección de datos. Este derecho-principio de la información en la Directiva tiene especial regula-

ción teniendo en cuenta, sí la información en el marco de esta *sociedad de la información* **[268bis]**, se ejercita en el caso de obtención de datos recabados del

propio interesado (art.10), o sí se trata de la información cuando los datos no han sido recolectados del propio interesado (art. 11) [269], pues en uno y otro caso, se arbitran peculiares garantías y derechos para el titular de los datos (v.gr. *habeas data* y sus derechos estructurales: acceso, rectificación, actualización y cancelación de datos, así como sus excepciones y limitaciones a los mismos [270] y el derecho de oposición

---

(268 bis) La información el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos (C.14), así como a cualquier información que se considere de la persona humana y sea tratada mediante procesos informáticos, electrónicos o telemáticos. Texto completo en la dirección electrónica: WWW. CC.CEC (DATABASE CELEX).

(269) Este punto se considera significativo al ser incluido como uno de los aspectos de interés incluidos en el Anteproyecto de reforma a la LORTAD, tras la transposición de la Directiva 95/46/CE, al ordenamiento jurídico español, que debe acaecer el 31 de Octubre de 1998. Vid. GUTIERREZ SANCHEZ, Pedro. *ANTEPROYECTO DE LA LEY ORGANICA POR LA QUE SE MODIFICA...* Ob, cit. p.5.

(270) La Directiva en el art. 12, estatuye los derechos estructurales del ejercicio del derecho de habeas data, tales como el derecho de acceso, rectificación, actualización y cancelación de datos personales que resultaren inexactos o imcompletos. Así como las acciones informáticas de supresión y bloqueo de datos. *DERECHO DE ACCESO*: Los Estados Miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: 1. La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refirieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; 2. La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; y 3. El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las denominadas decisiones individuales automatizadas (art. 15-1); b) En su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se haya comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el literal b, si no resulta imposible o supone un esfuerzo desproporcionado. Art. 13. *EXCEPCIONES Y LIMITACIONES*: 1.- Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el art. 6-1 (relativos a los principios de la calidad de los datos), art. 10 (Información en caso de obtención de datos recabados del propio interesado), art. 11-1 (Información cuando los datos no han sido recabados del propio interesado), y los arts. 12 (Derecho de Acceso) y 21 (Publicidad de los tratamientos), cuando tal medida constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) interés económico y financiero importante de un Estado miembro o de la Unión Europea (UE), incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia los literales c, d, y e.,; g) la protección del interesado o de los derechos y libertades de otros derechos. 2.- Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados con medidas o decisiones relativas a personas concretas, los Estados miembros, podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el art. 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas" Texto Completo de la Directiva 95/46/CE, en *WWW. CC.CEC* (Database Celex).

al tratamiento, previstos en los arts. 12 a 15, respectivamente de la Directiva); así como, las obligaciones y derechos para los sujetos involucrados en el tratamiento de datos, particularmente del responsable o encargado del tratamiento.

En el primer caso, es decir, cuando los datos personales sean recolectados del propio interesado, la Directiva suministra unas pautas mínimas que deben cumplir los sujetos involucrados en el tratamiento, pero particularmente el responsable del tratamiento o su representante, quienes deberán comunicar a la persona de quien se recaben los datos que le conciernen, por lo menos la siguiente información, salvo que ya hubiera sido informado de ello (más no, que no se dé por informado, por otros medios):

a) La identidad del responsable del tratamiento y, en su caso, de su representante; b) Los fines del tratamiento de que van a ser objeto los datos; c) Información acerca de los destinatarios o las categorías de destinatarios de los datos; el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada un negativa a responder; y la existencia de derecho de acceso y rectificación de los datos que le conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Se puede apreciar, como lo sostienen *Doumortier y Alonso* [271], la Directiva resulta en este aspecto nada formalista respecto del cumplimiento del deber de suministrar información al interesado, pues contiene una serie de elementos que garantizan una mayor flexibilidad, pues p.e., considera no necesario informar al interesado cuando él ya dispone de la información pertinente, no se requiere informar sobre la identidad del encargado del tratamiento. En fin, el régimen de información al interesado, es mucho menos costoso y complicado que el de la Ley Belga sobre tratamiento informatizado de datos, que obligaba a informar aún en los casos ahora exceptuados de la Directiva.

En el segundo caso, es decir, cuando la información de los datos no han sido

---

(271) DUMORTIER Y ALONSO BLAS, D. Ob. cit., pág. 11.

recolectados del propio interesado, aunque se aplica, a partir de la fase de registro de datos, previo almacenamiento de los mismos, por circunstancias temáticas la incluimos en esta fase inicial de recolección de los datos y haremos referencia puntal en los siguientes fases del proceso informatizado.

En desarrollo, de esta especial información cuando los datos no se recaben del interesado, el responsable del tratamiento o su responsable deberán, desde el momento del registro de los datos o, en caso de que piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la siguiente información, salvo si el interesado ya hubiere sido informado:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto de los datos; c) Información acerca de: 1. Las categorías de los datos de que se trate. 2. Los destinatarios o las categorías de destinatarios de los datos. 3. La existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se haya obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos legal respecto del interesado.

Se inaplicarán las anteriores informaciones, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En estos casos, estatuye la Directiva 95/46/CE, art. 11-2 *in fine*, que los Estados miembros establecerán “las garantías apropiadas”.

h) El principio del derecho de oposición del interesado al tratamiento de datos, constituye una garantía de protección máxima de los derechos y libertades fundamentales en manos del interesado cuando dichos datos personales han sido sometidos a tratamiento (informatizado o no). Este nuevo derecho de los titulares de datos (C.25 y 30., conc., art. 14 y 15 Directiva), junto con el ejercicio del derecho *de*

habeas data (acceso, rectificación y cancelación), constituyen la plataforma de defensa y protección que tiene toda persona dentro de la visión iusinformática de los derechos y libertades fundamentales, vale decir, de aquella parte de éstos y aquéllas en los cuales tiene incidencia los tratamientos y/o procesos informatizados en su pleno ejercicio, defensa y protección.

El derecho de oposición al tratamiento de datos, se manifiesta de dos formas: a) Como derecho de oposición al tratamiento propiamente dicho (art. 14); y, b) Como derecho de una persona a no verse sometido a una decisión individual informatizada con efectos jurídicos sobre aquella (art. 15).

El derecho de oposición del interesado, se ejercita por el interesado en cualquier momento del tratamiento de datos y "por razones legítimas propias de su situación particular" (o motivos fundados y legítimos relativos a su situación concreta. C.45), frente al tratamiento de cualquier dato personal que le concierna.

Ahora bien, se ejercitará este derecho de oposición en éstas condiciones por el interesado cuando: a) el tratamiento se requiere para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable o a un tercero a quien se comuniquen los datos; y , b) Cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran su protección. En caso de oposición injustificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos.

El titular de los datos, también podrá ejercitar el derecho de oposición, previa petición y sin gatos, al tratamiento de datos personales que le conciernen en los cuales el responsable prevea un tratamiento destinado a la prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, p.e., de carácter político. Caso, contrario, podrá solicitar se informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

El derecho del concernido de datos personales a verse sometido a una decisión con efectos jurídicos (art.15 Ibídem), consiste en que las personas no podrán verse sometidas a una decisión individual informatizada que tiene efectos jurídicos sobre aquélla, o cuando les afecte significativamente y se basa únicamente en un tratamiento informatizado destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

Sin embargo, el concernido puede verse sometido a una decisión individual informatizada, en los siguientes casos: a) Cuando se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; y, b) Cuando esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Es claro, como sostienen *Dumortier y Alonso Blas* [272], que la efectividad del derecho de oposición (en sus dos vertientes, agregamos) exige que se concrete un procedimiento de tutela del mismo, así como la inclusión de la tipificación de las conductas que le son contrarias y la correspondiente sanción.

4.5.1.2.3. FASES DE ALMACENAMIENTO, REGISTRO Y CONSERVACION DE DATOS.

Sea lo primero, insistir que algunos de los principios comentados para la fase inicial de recolección de datos son de aplicación a todo proceso informatizado de datos, y como tal, aplicables a las fases de almacenamiento, registro y conservación de datos. Estos son: a) El principio de lealtad y licitud de los datos; b) El principio de veracidad y exactitud de los datos; c) El principio de legitimidad del tratamiento de datos, que a su vez se compone de los principios del consentimiento del titular, finalidad de los datos y prevalencia de ciertos intereses públicos y privados; d) El principio de interdicción de tratamiento de datos personales pertenecientes a las “Categorías Especiales; e) Principio de información del interesado o titular de los datos; y e) El principio del derecho de oposición del interesado al tratamiento informatizado de datos.

En efecto, estos principios aplicables a todo el tratamiento, en el contexto de la Directiva se observa el énfasis que se pone a *la fase de registro de los datos*, quizá

---

(272) Ibídem., pág. 6

porque es a partir de ésta, donde se presenta esa visión paradójica del derecho-protegido y el derecho-vulnerado, devenida con, por y para la estructuración de un procedimiento informatizado de datos personales, por parte de los sujetos que intervienen en el tratamiento informatizado de datos (interesado, titulares de datos, terceros, responsables y encargados del tratamiento, etc); así como por la importancia, en el marco actual de la "sociedad de la información", a partir de la cual y tras el desarrollo de las nuevas tecnologías de la comunicación y la información (TIC), unidas a la informática, se pueden captar, transmitir, manejar, registrar, conservar y comunicar datos personales textuales, auditivos o sónicos o de imagen. Igualmente, porque día a día se van incrementando la formas de recolección de datos no directamente del interesado y se hace necesario establecer mecanismos de defensa, control y protección que garanticen al titular de esos datos una información precisa, clara e inequívoca (art.11), "desde el momento mismo del registro de los datos, o a más tardar, al comunicar los datos por primera vez a un tercero" (C.39 *in fine*), salvo que el interesado ya esté informado o "la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos" (C.40).

Como principios específico de la fase de registro, es *el principio de publicidad de los tratamientos.* En efecto, si los procedimientos de notificación previos al tratamiento de datos (art.18 Id.) a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva (C.48), la publicidad de los tratamientos constituye una pieza importante para ejercitar los derechos y cumplir los deberes quienes están involucrados en el susodicho tratamiento, así como para que "cualquier persona" pueda consultarlo, o para que se establezcan limites, restricciones o excepciones, según la categoría de los datos personales que se someten al tratamiento (art.21 Id.).

En *la fase de conservación de datos,* procede también, el *principio de identificabilidad de los interesados y de temporalidad de los datos*. En tal virtud, los datos personales se conservarán en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos (art.6 Id.).

4.5.1.2.4. FASE DE COMUNICACION DE DATOS: FLUJO O TRANSFERENCIA DE DATOS.

Como principios específicos para ésta fase, además de los principios generales del tratamiento de datos antes comentados en las otras etapas, podemos destacar el principio de confidencialidad y de seguridad del tratamiento y el de *la libre circulación de los datos* [273], los cuales guardan íntima relación cuando se somete a la fase de comunicación (por transmisión, cesión, difusión, etc) los datos personales previamente recolectados, almacenados, registrados y conservados. Cierto es que el principio de confidencialidad o secreto, como el de seguridad (técnica y jurídica) de datos se aplica a todas las fases del procedimiento, no es menos cierto que dicho principio se hace efectivo con mayor incidencia en la presente fase. Por esta razón, hemos incluido en este aparte su estudio.

El *Principio de confidencialidad y de seguridad del tratamiento.* Existe confidencialidad del tratamiento, cuando las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo pueden someter a tratamiento los datos a los cuales tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Por *el principio de seguridad del tratamiento*, el responsable del tratamiento

---

(273) Este capital principio aplicable en forma exclusiva a la fase de comunicación (por transmisión: emisión/recepción) de datos personales, es uno de los principales objetivos de la Directiva 95/46/CE., cuando expresa: "Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada de los derechos y libertades fundamentales de las personas físicas, y en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales" (art. 1). Más aún, "a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas

físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la Directiva 95/46/Ce, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad" (C.9).Texto Completo de la Directiva en *WWW.CC.CEC* (Database CELEX).

está obligado a aplicar las medidas técnicas (en consideración a los conocimientos técnicos y el coste de aplicación) y de organización adecuadas (es decir, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y la naturaleza de los datos por proteger), para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizado, *en particular cuando el tratamiento incluya la transmisión de datos de una red*, y contra cualquier otro tratamiento ilícito de datos personales (art.17-1 Id.).

El *principio de la libre circulación de datos*, desde la Recomendación de la OCDE de 1980, luego corroborada por el Convenio Europeo de 1981, ha constituido el eje central de la transmisión (emisión/recepción) de datos personales, a través de medios informáticos, electrónicos o telemáticos, porque se erige como el punto de equilibrio entre la protección de los derechos y libertades fundamentales de la persona humana y la liberación de obstáculos (técnicos y jurídicos) [274] para transferir datos entre los Estados miembros de la UE, o dentro del territorio de cada Estado entre organismos, personas jurídicas o físicas, públicas o privadas, sin que se eludan los mecanismos de seguridad, confidencialidad y protección de los datos, y a la vez, sin que representen un potencial riesgo a la vulneración de derechos y libertades fundamentales de la persona.

La Directiva 95/46/CE, con base en las normas comunitarias que le anteceden sobre la materia, regula en el Cap. IV, lo atinente a la "Transferencia de datos personales a países terceros", reduciendo así el ámbito territorial de las transferencias o flujos de datos a los estrictamente "internacionales", cuando se refiere a la transferencia entre países miembros o no de la Unión Europea (UE), siempre y cuando se reúnan unos requisitos de forma y de fondo.

---

(274) " Para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en

todos los Estados Miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones" (C.8). Texto Completo de la Directiva en *WWW.CC.CEC* (Database CELEX).

Las transferencias o flujos transfronterizos de datos personales son necesarios, principalmente según el C.56, para el desarrollo del comercio internacional, en tal virtud, las normas establecidas en la Directiva que prevalentemente se dirigen a la protección de las personas no se opone a la transferencia de datos personales a terceros países, siempre que garanticen un nivel de protección adecuado. El carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias.

La evaluación del nivel adecuado de protección garantizado por un país tercero, incluirá, entre otros aspectos: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países (art.25-2 Id.). Los Estados Miembros y La Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado. Una vez sea comprobado por la Comisión la falta de garantías por un país tercero, previo procedimiento establecido en la Directiva solicitará a los Estados que tomen las medidas necesarias para "impedir cualquier transferencia de datos personales" con dicho país.

Sin embargo, podrá realizarse transferencia de datos con terceros países que no garantizan un nivel de protección adecuado, siempre y cuando se reúnan los siguientes requisitos: a) el interesado haya dado su consentimiento inequívocamente; b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento

judicial; e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, f) la transferencia tenga lugar desde un registro público, en virtud de disposiciones legales o reglamentarias, esté concebida para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta (art. 26-1).

También se podrá transferir datos personales a "un tercer país que no garantice un nivel de protección adecuado..., cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas" (art. 26-2).

Los Estados miembros de la UE, tienen la obligación de informar la aplicabilidad de las anteriores excepciones sobre transferencias de datos personales, a la Comisión, la cual a su vez, adoptará las medidas adecuadas, a través de un procedimiento administrativo sumarísimo previsto en el art. 31 de la Directiva.

De esta forma, como lo sostiene *Dumortier y Alonso Blas* [275], la Directiva establece reglas claras con respecto a las transferencias internacionales de datos: total libertad dentro de la Comunidad y prohibición (con excepciones), cuando se trate de países terceros que no garanticen un nivel adecuado de protección.

4.5.2. LA DIRECTIVA 97/66/CE*, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI)* [276] *y las redes móviles digitales públicas.*

La fase informatizada de comunicaciones (o "telecomunicaciones" como prefiere, la Directiva) de datos personales con el desarrollo constante y revolucionario de las nuevas tecnologías de la información y comunicación

(275) DUMORTIER Y ALONSO BLAS, D. Ob. cit., pág. 11.

(276) El Parlamento ha subrayado la importancia de proteger los datos personales y la intimidad en las redes de telecomunicaciones, especialmente en relación con la introducción de la Red Digital de Servicios Integra dos (RDSI). El Consejo de la UE, en la Resolución de 18 de Julio de 1989, ya había hecho énfasis en la mencionada protección y sobre una mayor coordinación estatal sobre el tema de la RDSI. En la Parte IV. Punto 5 y ss., haremos comentarios puntuales sobre el tema

(TIC) [277] , día a día, se va super especializando cara a los intereses, derechos y libertades fundamentales dignos de protección y garantía por parte del Estado e incluso de los mismos particulares; así como el de preservar los principios de *la libre circulación de los datos* y la confidencialidad de las comunicaciones [228] que transiten entre los Estados de la UE, conjuntamente con los cada vez, paradójicamente por el mismo avance, espectros de riesgo y vulnerabilidad que crecen geométricamente y se concretan; entre otras actividades, en el acceso, la transformación o la interceptación no autorizada de datos personales y continentes en bases de datos públicas o privadas, a través de medios muy sofisticados de tipo informático, electrónico o telemático. Acciones humanas indebidas, abusivas o ilegales que generan reproche social y normativo que en España van, desde las sanciones administrativas por infracciones (o contravenciones) al régimen del tratamiento informatizado de datos personales, previsto en la LORTAD, hasta las sanciones penales por estar incursos en formas delictuales contra los derechos y libertades fundamentales (entre ellos, la intimidad, la imagen y el honor, la información, etc.) [279].

La Directiva 97/66/CE, constituye una norma jurídica comunitaria que refuerza,

---

(277) En efecto, son los Estados de la UE, quienes mediante sus disposiciones normativas, garanticen, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicaciones y de los servicios públicos de telecomunicaciones. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente (C.5).

(278) El Parlamento Europeo y el Consejo de la Unión Europea (UE), consciente de dichos avances y de que la Directiva 95/46/CE, constituye un buen instrumento, pero jamás suficiente, de defensa de los derechos y libertades fundamentales de la persona humana, ha venido trabajando una propuesta común que se concre-te en una Directiva Comunitaria que refuerce y especialice la protección de esos intereses y derechos, ya que "en la actualidad están apareciendo en la UE nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios; que el desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de telecomunicaciones; que el desarrollo transfronterizo de estos servicios, como el vídeo por pedido o la televisión interactiva, depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad" (C. 2). Texto Completo de la Proposición Común (CE) No. 57/96, relativa a la protección de los datos personales y de la intimidad en relación con el sector de las telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales, en WWW. *CC. CEC (Database CELEX).*

(279) En la Parte IV, hablaremos sobre estos temas. Así mismo plantearemos a título de ensayo el delito que llamamos de *datos personales registrados en forma automatizada contra la intimidad*. Este consta de dos partes: una, configurada por el acceso, utilización y alteración de los datos (parte *ab initio del tipo*); y otra,

estructurada por la interceptación o intervención de los datos, por medios informáticos, electrónicos o telemáticos (parte *in fine del tipo*). Todo ello, con base en el estudio y análisis del actual Código Penal (Libro II, Delitos y Penas: Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio) y las normas extrapenales como la LORTAD y las Directivas 95/46/CE y 97/66/CE, sobre telecomunicaciones e intimidad.

amplía y concreta el régimen previsto en la Directiva 95/46/CE, sobre protección a los derechos y libertades fundamentales (particularmente, el derecho a la intimidad) de las personas humanas, cuando sus datos han sido tratados con medios informáticos, electrónicos o telemáticos, haciendo énfasis en la fase de transmisión (emisión/recepción) de datos. En tal virtud las normas de la Directiva 95/46/CE, se aplicarán por extensión, en cuanto a los recursos judiciales, régimen de responsabilidad y sanciones (art. 14-2); así mismo se podrá limitar el alcance de las obligaciones y derechos previstos en los denominados por la Directiva 95, "Principios relativos a la calidad de datos" (art.5 y 6), y los datos de "categorías especiales de tratamiento" (art. 8-1 a 8-4), cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicaciones (art. 14-1).

La Directiva consta de una parte interpretativa y hermenéutica (26 considerandos) y un cuerpo normativo, con los siguientes temas: Objetivo y ámbito de aplicación (art. 1), Definiciones (art. 2), Servicios regulados (art.3), Seguridad (art.4), Confidencialidad de las comunicaciones (art. 5), Tráfico y facturación (art.6), Facturación desglosada (art. 7), Presentación y limitación de la identificación de la línea llamante y conectada (art. 8), Excepciones (art. 9), Desvío automático de llamadas (art.10), Guías (11), llamada no solicitada (art. 12), Características técnicas y normalización (art. 13), Extensión del ámbito de aplicación de determinadas disposiciones de la Directiva 95/46/CE (art. 14), Aplicación de la Directiva (art.15), y Destinatarios (art. 16).

4.6. AUSTRALIA: LEY DE LA INTIMIDAD Y LA PROTECCION DE LOS DATOS: BILL AUSTRALIANA DE 1994.

The Privacy and Data Protection Bill 1994 (NSW), [280] es una de los más recientes Estatutos normativos de corte anglosajón que regulan la protección de los derechos fundamentales de la persona humana, especialmente el derecho a la

intimidad, cuando los datos personales han sido sometidos a un proceso informatizado, con medios informáticos, electrónicos o telemáticos.

---

(280) Texto original y completo en inglés en : WWW. AUTLI. EDU. AU. (Database de la Universidad de Australia).

finales remisorias a otras leyes aplicables subsidiariamente a ésta, tales como la Ley de la Intimidad Australiana de 1988 (*Privacy Bill 1988*); entre otros temas, sobre el "Comisionado para la protección de la Intimidad" (*Privacy Commissioner*), el Consejo Consultivo de la protección de la Intimidad (Privacy Advisoy Committee) , la regulación de la libertad de información (*Freedom of information Act 1989*) **[281]** y la Ley de regulación del Defensor del Pueblo (*L´Ombusdman Act 1974*). Cada parte, a su vez, contiene divisiones, secciones y artículos.

LA PARTE PRIMERA. PRELIMINARES.

En esta parte se hace referencia; entre otros, a los siguientes temas:

1. *OBJETIVOS DE LA BILL AUSTRALIANA DE 1994.* Los cuales se resumen así: a) Estatuir los mecanismos de protección de los titulares de los datos personales en las diferentes fases del tratamiento informatizado, y sobre todo, en la etapa de recolección, como en la posterior utilización, consulta, divulgación o descubrimiento de dicha información personal, tanto realizadas por las autoridades Estatales, como por personas u organismos del sector privado, b) Atribuir funciones específicas a la oficina del Comisionado para la protección del derecho a la Intimidad, sobre éstas materias, c) Organizar el Comité Asesor para la protección de la Intimidad; d) Derogar las normas contrarias, en especial, las referidas al Comité Asesor previstas en la "Bill" de 1975.

. 2. DEFINICIONES TECNICO-JURIDICAS. Contiene un amplio glosario de términos jurídicos y técnicos (iusinformáticos) utilizados en todo el texto normativo de la Bill 1994. Entre otros, destacamos los siguientes:

a) *Recolector de datos* ("Collector"). Personas, autoridades u organismos con funciones públicas o privadas, o en su caso, sus representantes, dedicados a la colecta de información de carácter personal. Estas funciones incluyen derechos, deberes y obligaciones para quienes las ostentan.

(281) Según el art. 51 de la Bill 1994, no será objeto de requerimiento o descubrimiento de información, aquellos conceptos y disposiciones que regulan la información general e incluso personal que no afecta la intimidad ni los datos personales informatizados y previstos en La Ley de protección a la información Australiana de 1989.

b) Jefe de una Autoridad Pública. Se utiliza para referirse a los Jefes de una oficina administrativa, Autoridad Gubernamental local, Directores del Servicio de Educación, Servicio de Policía, etc.

c) *Información personal*. Cualquier información u opinión sobre una persona, incluida la que hace parte de un banco de datos, sea verdadera o no, bien sea almacenada en forma material o con medios informáticos. La información personal identificará a una persona o permitirá razonablemente identificarla.

d) *El Comsionado para la protección de la Intimidad* . Es la autoridad encargada de salvaguardar, proteger y hacer cumplir las normas sobre la protección del derecho a la intimidad cuando se sometan a tratamiento informatizado los datos personales.

e) *Registro Público*. Es el asiento o registro de una información personal ante las personas o autoridades competentes, cuando la ley así lo requiere, para publicitarla, ponerla a disposición o consulta de aquellos que están habitados por la ley para hacerlo.

f) *Unidad de información personal informatizada* ("Record"). Esta unidad, puede esta contenida, a los efectos de la Bill 1994, en: 1. Documentos. Incluye además de los tradicionales documentos, los definidos como tales, en la *Act 1987* v.gr. Los discos informáticos, cintas u otros artículos que pueden almacenar o grabar sonido, imágenes o mensajes capaces de ser reproducidos por emisión o recepción; b) La información contenida en una fotografía o representación pictórica de una persona, pero no incluye la que se halle en una revista, libro, periódico u otra publicación que son o están, por regla general, a disposición del público, o aquellas imágenes de una persona que se hallan en los Archivos del Estado ("State Archive". Previstos en The Archives Act 1960), tales como en Bibliotecas, Galerías de Arte o Museo y en los cuales se tiene el propósito referenciales o de investigación, como

para el estudio, la realización de escritos o artículos, para la exhibición, o finalmente para la transmisión electrónica o por cable teniendo en cuenta los anteriores fines.

g) *Vigilante de los datos o Informaciones Personales* ("Record-Keeper"). Es la persona u organismo responsable de la posesión y administración de una información personal. El vigilante de los datos, también se le conoce como Vigilante o responsable de los registros. Este puede ser público o privado, según la información personal que posea o administre.

PARTE II. VIGILANCIA Y PROTECCION DE LOS DATOS O INFORMACIONES PERSONALES.

Esta parte se subdivide en cuatro (4) divisiones, que tratan a su vez, los temas siguientes: a) Tratamiento de información en el Sector Público; b) Los Códigos de Protección de los Datos personales (*Data protection Codes*: En el Sector Público [282] y en el Sector Privado [283]); c) Los Registros Públicos; y d) Los principios de protección

---

(282) La Bill Australiana de 1994 en la División II, artículos 10 a 12 se refiere a estos temas. "Division 2. Data protection codes. SECT 10. Data protection codes must be prepared for public sector. 10. (1) For the purpo-se of better protecting individual privacy, a data protection code relating to the collection, use and disclosure, and procedures for dealing with, personal information held by a public authority must be prepared y Th heda of Th publica adherida ad adoptad y Th publaca adhegida. (2) Th conde mus be preparado ad adoptad no later Th 12 montas afer Th commencement of this section or the establishment of the authority, whichever is the later. (3) This section applies to personal information about any persons, including the employees of public authorities. SECT 11. Requirements for public sector data protection codes. 11. (1) A data protection code of a public authority must: (a) specify procedures for dealing with personal information; and (b) specify conditions to be imposed as to the disclosure by the Archives Authority of New South Wales of public records (within the meaning of the Archives Act 1960) that are records of the public authority or information contained in them; and (c) be submitted to the Privacy Commissioner for review before adoption. (2) The code must, in relation to procedures for dealing with personal information, conform, so far as is reasonably practicable, to the data protection principles set out in Division 4. (3) That part of the code relating to conditions to be imposed on the Archives Authority of New South Wales must conform, so far as is reasonably practicable, to Principle 10 of the data protection principles. (4) Despite subsections (2) and (3), a code may permit personal information to be disclosed by the public authority to another public authority for the purposes, and in the circumstances, specified in the code. (5) Before a code is adopted, the head of the public authority must consider the findings of the review of the code by the Privacy Commissioner. SECT 12.Amendment of public sector data protection codes. 12. (1) The head of a public authority may, from time to time, amend its data protection code and must submit the amendment to the Privacy Commissioner for review before adoption. (2) Before the amendment is adopted, the head of the public authority must consider the findings of the review of the amendment by the Privacy Commissioner". Texto completo en: *WWW.AUSTLI. EDU.CO*. (Database de la Univ. De Australia).

(283) Códigos de protección de datos en el Sector Privado: "SECT 13. Private sector data protection codes. 13. (1) The Privacy Commissioner may, at the request of a person or body that is not a public authority, prepare a data protection code relating to the collection, use and disclosure, and procedures for dealing with, personal information held by the person or body for adoption by the person or body. (2) A person or body that is not a public authority may prepare and adopt a data protection code relating to the collection, use and disclosure, and

procedures for dealing with, personal information held by the person or body and may submit the code to the Privacy Commissioner for review. SECT 14. Requirements for preparation of private sector data protection codes. 14. (1) In preparing a data protection code under this Division for a person or body that is not a public authority, the Privacy Commissioner must specify procedures for dealing with personal information. (2) The code must conform, so far as is reasonably practicable, to the data protection principles set out in Division 4. SECT 15.Amendment of private sector data protection codes. 15. (1) A person or body that is not a public authority may, from time to time, amend its data protection code and must submit the amendment to the Privacy Commissioner for review before adoption. (2) Before the amendment is adopted, the person or body must consider the findings of the review of the amendment by the Privacy Commissioner. SECT 16.Exemptions from public and private sector data protection codes. 16. (1) The Privacy Commissioner may, at the request of the head of the public authority or other person or body by or for whom a data protection code is or is to be prepared, exempt personal information or classes of personal information or a person or any classes of persons from de los datos personales.

Los principios de protección de los datos aplicados a las diferentes fases del procedimiento informatizado en la *Bill 1994* de Australia, están previstos en el artículo 21 de la siguiente forma:

1. *Principio de finalidad en la recolección de los datos*. Los datos personales deberán ser recolectados por las personas u organismos (públicos o privados) para los fines o propósitos previstos en las leyes y directamente relacionados con sus funciones o actividades. La información personal, por tanto, para cumplir estos fines y propósitos no será recogida por medios ilegales o injustos.

2. *Principio de información de los datos personales al concernido*. El interesado podrá solicitar directamente la información de los datos personales que le conciernen, a quienes la han recogido (Colectores), excepto si autoriza a otra persona para que descubra o divulga la información de conformidad con los principios de la *Bill 1994* de Australia y siempre y cuando sea utilizada para ser incluida en un registro o una publicación disponible o accesible al público y se tomen por parte del Recolector todas las medidas de seguridad seguidas en la recolección, y siempre y cuando sea informado previamente al concernido, si fuere posible, sobre los siguientes aspectos: 1) Propósitos de la recolección; 2) Sí ha sido autorizada por la ley; 3) La naturaleza obligatoria o voluntaria de la recogida de datos; 4) Los efectos en el concernido al proporcionar parte o toda la información solicitada; 5) La existencia de los derecho de acceso y rectificación de los datos (*habeas data*), y si fuere el caso, la cancelación; 6) El nombre y dirección del Vigilante y Protector de los datos; y, 7) Cualquier otra informa

---

Continuación de cita No. 283

any or all of the provisions of the code. (2) A data protection code must identify any personal information or persons or classes of personal information or persons exempted from any or all of the provisions of the code. (3) An exemption may be revoked or varied at any time by the Privacy Commissioner on request by the head of a public authority or other person or body by or for whom a data protection code is or is to be prepared. (4) An exemption in a data protection code of a public authority may be revoked or varied at any time by the Privacy Commissioner on the Commissioner's own initiative. (5) The Privacy Commissioner is to review each exemption given by the Commissioner if it is still in force 3 years from the date it is given or was last reviewed. The review is to be undertaken as soon as possible after the end of the period of 3 years from that date". Texto completo en: *WWW.AUSTLI. EDU.CO*. (Database de la Univ. de Australia).

ción sobre las personas, organismos o agencias que tengan actividades de recolección de información personal y estén relacionadas con sus datos personales.

3. *Principio de solicitud de información disponible o de acceso al público.* Los datos personales recogidos en un registro o disponibles en una publicación de acceso al público, pueden ser solicitadas por el recolector de los mismos, siempre que la información sea pertinente, no exceda los propósitos para los cuales fue recabada, sea exacta, completa y actualizada. Igualmente que la información no constituye un obstáculo irrazonable en los asuntos de la persona concernida

4. *Principio de almacenamiento y seguridad de la información*. El vigilante del registro de los datos personales ejercerá el control de los mismos. En virtud, los datos serán protegidos para que: a) sean posteriormente utilizados con los mismos propósitos explícitos y legales para los que fueron almacenados; b) Sean igualmente utilizados en forma adecuada, pertinente y en forma no excesiva respecto de los propósitos con los que se recabaron; c) Sean procesados o tratados justa y legalmente; d) Sean almacenados por un espacio de tiempo necesario concordante con los fines y propósitos de dicho almacenamiento; e) la protección del almacenamiento se extienda a las medidas de seguridad necesarias contra el adquisición, la pérdida, el acceso desautorizado, uso, modificación, descubrimiento o divulgación, y contra cualquier otro mal uso de datos; y, f) Si fuese necesario, para evitar un uso desautorizado o descubrimiento de datos, será implementado un servicio especial de vigilancia y protección de datos, según lo considere razonable el Vigilante del Registro de datos.

5. *Principio de información relacionada con los datos personales registrados por el Vigilante de los mismos.* El vigilante podrá informar a cualquier persona cuando se lo solicite acerca de la existencia de la posesión y control de cualquier dato personal que le concierna y si existe algún otro dato adicional que se

relacione con el solicitante. En tal virtud, le informará sobre: a) la naturaleza de la información; b) los propósitos principales para los cuales será utilizada la información; c) los trámites que debe seguir para hacer uso y ejercicio del derecho de acceso a los datos personales o registros.

Sin embargo, el Vigilante de los datos, podrá negarse a suministrar información en las condiciones anteriormente descritas, si el solicitante no está autorizado por la ley o documento.

El Vigilante de los datos personales, deberá mantener y poder informar de: a) la naturaleza de los datos personales; b) las fuentes de información que suministraron los datos; c) los propósitos para los que fueron recaudados los datos, así como la autoridad que tiene su posesión y control; d) el propósito específico de almacenamiento de cada dato personal; e) las clases de personas acerca de las cuales se almacena un dato; f) el período de tiempo por el que se almacena un dato; g) las personas que son titulares para ejercer el derecho de acceso a la información personal y las condiciones bajo las cuales ostentan dicha titularidad; h) los trámites que deben seguir los titulares de los datos para ejercer el derecho de acceso a los datos que les conciernen.

El Vigilante de los datos mantendrá un registro de los anteriores datos, a fin de ponerlos a disposición de inspecciones realizadas por autoridades (administrativas o judiciales), cuando así se lo requieran o por disposición legal. Así mismo, para enviar una copia en el mes de junio de cada año, con destino al Comisionado de Protección para la Intimidad.

6. *Principio de Acceso a los datos personales registrados por el concernido*. El Vigilante de los datos, permitirá el acceso a los datos personales que le conciernen, sin demora y sin gasto alguno. El acceso no se permitirá a la totalidad de los registros o informaciones almacenadas y registradas, si no es con autorización legal o documento que así lo acredite.

7. *Principio de alteración de los datos personales.* El Vigilante de los datos, podrá proceder a las correcciones apropiadas, cancelaciones y modificaciones a los datos en circunstancias legales y que aseguren la integridad de los datos, siempre

que el dato no sea exacto o completo o, no esté conforme a los propósitos para los cuales fue recabado y almacenado.

Si los datos personales han sido corregidos, anulados o agregados de conformidad con las razones y circunstancias anteriores, el titular de los datos o concernido será informado y notificado de dichas alteraciones. Sin embargo, este principio podrá ser limitado conforme a la aplicación de una ley estatal, cuando se trate del ejercicio de derechos contenidos en un documento que se requiera corregir o enmendar. Es el caso de los documentos en los cuales el Vigilante de los datos no esta legado para enmendarlo con correcciones, adiciones o cancelaciones, de conformidad con la petición (o demanda) de la persona concernida y las previsiones legales de la Bill 1994.

8. *Principio de Veracidad de la información personal antes de su utilización.* El Vigilante de los datos no permitirá el uso de los datos, sin previamente tomar las medidas necesarias para asegurar que la información personal está conforme a los propósitos para los cuales se solicita su utilización, así como que la información es pertinente, exacta, actualizada y completa.

9. *Principio de límites para el uso de la información personal (datos).* El Vigilante de los datos, no permitirá el uso de la información personal con propósitos diferentes para los cuales fue recabada y almacenada, salvo que: a) la persona concernida haya dado su consentimiento para el uso de conformidad con dicho propósito; b) el Vigilante de los datos presuma razonablemente que con la utilización de dicha información personal se puede prevenir o disminuir una amenaza seria e inminente a la vida o a la salud de individuo concernido u a otra persona; c) el uso de la información personal es necesaria para la investigación (judicial o policiva) de conformidad con la Ley Penal o Ley de Impuestos, o para la protección de un crédito público; d) el uso de la información personal sea requerida por autorización legal; y, e) el uso de la información personal está relacionado directamente con el propósito para el cual fue recabado.

10. *Principio de los límites al descubrimiento o divulgación de la información personal (datos).* El vigilante de los datos, no permitirá el descubrimiento de la información personal a una persona, organismo o agencia de

recolección de datos, a menos que: a) la persona concernida haya estado informada previamente de dichos propósitos; b) la persona concernida haya dado su consentimiento al descubrimiento; c) el Vigilante de los datos presuma razonablemente que el descubrimiento de información personal es necesario para prevenir o disminuir una amenaza seria e inminente a la vida o a la salud de la persona concernida u a otra persona; d) el descubrimiento es requerido o autorizado mediante ley estatal; e) el descubrimiento es necesario para una investigación (administrativa o judicial), según la Ley Criminal o Ley de Impuestos, o para la protección de un crédito público.

El uso que se debe dar a la información personal descubierta en las circunstancias y condiciones anteriores será única y exclusivamente el que corresponda al propósito para el cual fue solicitado. En caso del descubrimiento para investigaciones se hará constar en una nota al margen el uso específico de la información personal.

11. *Principio de los límites en el uso de "información personal sensible" ("Certain Information* [284] *")* . Muy a pesar de los dos principios anteriores (9 y 10), la información personal relacionada con el origen étnico o racial, las opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos o, los relativos a la salud o vida sexual, no podrán ser descubiertas por el Vigilante de los datos, sin el consentimiento expreso y escrito, libremente otorgado por la persona concernida, excepto si está autorizado por ley.

La información personal relacionada con la historia delictiva de una persona, sólo podrá procederse a su descubrimiento, cuando sea requerida o por autorización legal o por la Bill 1994.

PARTE III. EL COMISIONADO PARA LA PROTECCION DE LA INTIMIDAD.

Contiene dos Divisiones: a) Sobre las quejas e investigaciones; y b) Los Informes.

Enunciaremos algunas de las funciones principales del Comisionado en relación con la protección de los datos del concernido, previstas en el art. 22 de la Bill 1994. Estas son: a) Promover la adopción de los principios de protección de los datos y las pautas para lograrlo con miras a promoción de la Intimidad tanto en el sector público como en el sector privado, b) Dirigir las investigaciones en materia de protección de los datos y la intimidad de las personas, c) Proporcionar ayuda a las autoridades públicas que lo requieran sobre los *Códigos de Protección de los datos*, d) Suministrar consejos a cualquier persona acerca de la necesidad o conveniencia de implementar instrumentos legislativos, administrativos o de otra índole en interés de la intimidad de las personas, e) Supervisar los desarrollos tecnológicos TIC e informática

---

(284) La Bill 1994 de Australia, emplea la terminología de "Certain Información" (información segura), para referirse a la información personal sensible o "Datos sensibles".

e informar a los interesados para minimizarlos, si éstos pudieran tener un impacto adverso en la protección de los datos y a la intimidad, f) Recibir e investigar y, si fuese procedente, conciliar las quejas sobre el uso y descubrimiento de la información personal (pública o privada) o de otras vulneraciones a la intimidad, g) Redactar un informe Anual sobre las quejas y recomendaciones al Ministro. Así mismo, presentar un informe especial al Parlamento, cuando sea requerido por éste; y, h) Preparar y publicar un catálogo sobre los registros que llevan los Vigilantes de los datos, con la información relacionada en el principio 5, en particular sobre las autoridades públicas allí relacionadas.

PARTE IV. EL COMISIONADO PARA LA PROTECCION DE LA INTIMIDAD.

En esta parte de la *Bill 1994* de Australia, se hace referencia a las calidades requeridas para ser nombrado como Comisionado de la protección de la Intimidad, el personal adscrito a dicha dependencia, cuando se trate en el sector público, así como las funciones especiales y generales y los poderes de delegación para cumplimiento de las mismas, aprobadas por el Ministro correspondiente.

PARTE IV. EL COMITE ASESOR PARA LA PROTECCION A LA INTIMIDAD.

Hace referencia al Comité Asesor para la protección a la intimidad, designación de los miembros que lo componen y funciones. Su función prioritaria es aconsejar al Comisionado para la protección de la intimidad en las materias relacionadas con sus funciones (tanto en el sector público como privado), así como recomendar puntualmente los aspectos (técnicos o jurídicos) para que sean incluidos por éste en la protección de los datos personales y la intimidad.

PARTE VI. DISPOSICIONES VARIAS. ("*Miscellaneous*").

Contiene las disposiciones generales y funciones previas del Comisionado para la protección a la intimidad sobre el "Procedimiento de Contravenciones" o de infracciones a la Bill 1994 (las cuales se relacionan taxativamente en el art. 49), tales como el envío de la información precisa para que sea adelantada una investigación por un "*Tribunal Local*" (Local Court), así como la aplicación de las excepciones para descubrir información personal en estos casos.