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.

PARTE III

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

*Ad porta*s del siglo XXI, vivimos en una sociedad típica y tópicamente caracterizada por los nuevos mecanismos, procedimientos, equipos y aparatos electromagnéticos que han reelaborado el concepto primigenio de la información y la comunicación. Somos libres y esclavos, en la *sociedad del chip:* las nuevas tecnologías aplicadas a todos los ámbitos de la vida humana, particularmente, los que se refieren a los diversos medios personales y sociales de comunicación; los que hacen relación a las fuentes de adquisición, consulta y divulgación de una información de carácter particular, oficial o institucional; y finalmente, los generados en las relaciones entre individuos, de estos con los Estados e incluso entre Estados mismos.

En esta Parte del trabajo, demostraremos las anteriores premisas generadas por el tópico de la información a través de medios electromagnéticos, considerada, hoy por hoy, más poder que nunca. Así mismo, a título de ensayo, la proposición de un procedimiento informatizado de datos personales viable en cualquier Estado que dispone de normas jurídicas generales o especiales sobre tratamiento de datos.

1. LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION. LAS NUEVAS RELACIONES ENTRE EL INDIVIDUO Y EL ESTADO.

La informática jurídica o *iusinformática* [1], es el resultado de la unión del derecho y la informática. En efecto, el derecho y en particular, el derecho público occidental, ha estudiado amplia como fructíferamente todo lo concerniente a los derechos fundamentales; entre otros, el de la intimidad personal y familiar (en particular

---

(1) Mi trabajo, *LA CONSTITUCION DE 1991 Y LA INFORMATICA JURIDICA.* Ed.UNED, Universidad de Nariño, Pasto (Col), 1997, págs. 43 y ss.

los datos personales iusinformáticos constitutivos de la intimidad), el de habeas data (acceso, actualización, rectificación y cancelación de datos personales del concernido, titular o persona interesada) y el de la información (por activa y por pasiva). De otra parte, *la informática*, entendida básicamente como el conjunto de reglas, principios y procedimientos teórico-técnicos que incardinados estudian las formas de recolección, selección, organización, tratamiento, almacenamiento y transferencia (por cesión o consulta) de los datos o informaciones de toda clase, tipo, modalidad o fin, llevados a cabo por medios informáticos, electrónicos o telemáticos.

Un ser humano desde antes de nacer, luego con su nacimiento, crecimiento, desarrollo, muerte, y aún después de ésta, produce una serie de actos, hechos, sucesos susceptibles de documentación (certificados de cualquier tipo y finalidad, registros públicos y privados, obligaciones y contratos, etc); en fin, de informaciones y datos personales, familiares y sociales, los cuales, en mayor o menor grado son sujeto u objeto del derecho y en mayores proporciones de la vida cotidiana, al ser puros y simples y reveladores de la venida, paso y extinción de la *vitae humanum*.

El status del *nasciturus* de la persona natural o física y el del *post mortem* en el derecho genera una gran cantidad de información o datos de carácter personal y familiar, tanto escritas, gráficas, auditivas, video auditivas como producidas, captadas, reproducidas, transferidas o consultadas por cualquier medio, dispositivo, aparato mecánico, eléctrico o electromagnético conocido o conocible, muchos de los cuales tienen relevancia en el derecho, dependiendo de diferentes variables que van desde las estrictamente biológicas (v.gr .nacimiento), pasando por las simplemente materiales u objetivas hasta las más sofisticadas que actualmente se conocen, cuando crean, modifican o extinguen situaciones jurídicas individuales o concretas, o generales y abstractas, produciendo derechos, deberes y obligaciones para una persona. Una auscultación médica mediante la técnica de rayos X o cualquiera otra de índole computarizada (p.e. TAC) o de examen de líquidos humanos (orina, sangre, semen, etc) o incluso de partes del cuerpo humano (v.gr. huellas digitales o plantares); cualquier número o símbolo que identifique o se le asigne a una persona (v.gr. documento de identidad personal, profesional, documento de conducción, etc); la información sobre la raza, origen étnico, color, religión, edad o estado civil o sobre la educación, su historial laboral, delictivo, incluso las ideas u opiniones personales sobre otra persona, salvo las vertidas con ocasión de un concurso, premio o subvención según la *Act Privacy Canadiense*; entre muchas otras relacionadas en un gran listado que no distingue categorías especiales entre aquéllas, constituyen información personal, entendiendo como tal, la que le concierne a una persona, cualesquiera sean los mecanismos o tecnologías de las que se obtengan o graben [2].

La Ley Orgánica de regulación del "*Tratamiento automatizado*" de los datos de carácter personal y familiar de España (LO 5/1992, Oct.29), define a los "datos de carácter personal" como "*cualquier información concerniente a personas físicas identificadas o identificables*" (art.3.a),). Persona identificable, según la Directiva 95/46/CE, es "*aquella a quien puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social* (art. 2.a.).

En términos iusinformáticos , las expresiones "*cualquier información*" deben interpretarse como una unidad de datos (sea textual, gráfica, imágenes fijas o móviles, auditivas o vídeo-auditivas) representada en forma o por el *sistema binaria* (ceros y unos: 0-1 [3]) en el tratamiento electromagnético o computarizado (especialmente en su almacenamiento --storage-- y teletrasmisión en unidas compatibles de discos fijos o "duros", de discos de acetato o "flexibles", o de discos compactos "Compac Disc" o medios informáticos de software o hardware, respectivamente) y relacionada con una persona natural o física. La información recolectada, seleccionada, organizada, proce sada, almacenada y recuperada mediante consulta o transferencia, total o parcialmente por medios no simplemente "automatizados", sino por dispositivos o aparatos eléctri tricos, electrónicos o electromagnéticos (telecomunicaciones y ordenadores, básicamente).

En consecuencia, en el siguiente aparte del trabajo expondremos las relaciones, ventajas, inconvenientes y prospecciones que presenta actualmente el estudio de la informática jurídica, los llamados "*datos de carácter personal y familiar*" y el procedimiento informatizado o electromagnético de los mismos, especialmente en sus

---

(2) LDPIC o La Ley de Protección a la intimidad canadiense, contiene un relación detallada de los actos, hechos y sucesos constitutivos de *información personal*. El art. 3 no es una cláusula cerrada o taxativa de estos supuestos sino meramente enunciativa. En la parte IV del trabajo, profundizaremos sobre el tema en el aparte.5.5.3.3 y siguientes, sin perjuicio de lo que comentemos aquí. El texto completo de la ley en: WWW.UMONTREAL.EDU.CA. Biblioteca Virtual de derecho de la Universidad de Montreal, Canadá. Vía internet. 1998.

(3) Los ordenadores o computadores trabajan en sistema binario (0-1) y no decimal. Esto significa que lo hacena través de "cambios e impulsos electrónicos" que compilan todas las operaciones, funciones y procedimientos lógicos en su memoria. Esto se conoce como "lenguaje de máquina". El computador cuando destella ceros, significa que hay ausencia de impulso, y si son unos, hay presencia de éstos. Esta función es similar a la de un commutador eléctrico que a la presión digital deja o no pasar electricidad, pero cada tiempo es diferente. AA. VV. CONOZCAMOS AL COMPUTADOR. Ed. Kernel, Bogotá, 198(?), pág. 1.

etapas de almacenamiento y transferencia, pues es aquí donde surge; por una parte, esa amalgama compleja de las nuevas tecnologías de la información y de la comunicación (TIC) que unen los últimos avances de las telecomunicaciones, esas redes globales, sin límites geográficos

que conforman con el no menos significativo y cada día más sofisticado mundo de los ordenadores y la electrónica; y por otra, el mayor o menor nivel de riesgo, vulnerabilidad frente a la actividad estatal o particular de protección y garantía a los derechos y libertades públicas e intereses legítimos que ese especie de matrimonio de las comunicaciones con el amplio espectro de la electrónica y los ordenadores, representan en la sociedad actual.

Para algunos [4], las expectativas, controversias y posibles soluciones que desencadenan las nuevas tecnológicas TIC, plantean, cuando menos, el rediseño de ciertos paradigmas de la humanidad que por siglos han guiado la actividad del ser humano, tales como la escritura y subsiguiente el denominado mundo de la impresión, por el que hoy, podríamos llamar del *universo digital de la información y comunicación.*

Sabemos que por siglos ha dominado el quehacer de la humanidad, la llamada la *cultura de la escritura*, precedida de la denominada *cultura de la impresión* y en particular, la lógica generada por el texto impreso desde que *Juan Guterberg* inventara "La Imprenta" y pudiera el hombre perpetuar sus ideas, opiniones y pensamientos y transmitirlos a otros, en principio en número limitado de copias idénticas del original y luego con el avance de las técnicas tipográficas y litográficas en miles de millones por el mundo. El hombre pudo así informar y ser informado de alguna cosa, suceso o historia. La información impresa con forma y contenidos (textuales y/o gráficos, únicamente) limitados al texto, artículo, folleto o al libro mismo produjo una lógica propia, una información individual, pasiva y algunas veces grupal, pues estaban situadas en sitios fijos e identificables (bibliotecas reales, estudios, etc públicos o privados) y muchas veces inapropiadas para todos, tanto locativa como temporalmente.

---

(4) KATSH, Ethain. *RIGHTS , CAMERA, ACTION: CYBERSPATIAL SETTINGS AND THE FIRST AMENDMENT.* Professor of Legal Studies, University of Massachusetts at Amherst; B.A. 1967, New York University; J.D. 1970, Yale University. Texto completo en: *WWW.UMONTREAL.EDU.CA.*

Con el advenimiento de las nuevas tecnologías TIC, unidas al mundo de la electrónica y particularmente de los ordenadores, surge una nueva lógica en el fenómeno de la información y la comunicación, una nueva cultura dominada por la electrónica que guía las actividades de las personas en todos los sectores incluidos el derecho, las relaciones entre los particulares, entre el ciudadano y el Estado e incluso entre los Estados, eufemísticamente se catalogó por los

norteamericanos como *cultura electrónica* ("*The electronic culture*" [5]), que como piedra de toque extrapiramidal,
provee de argumentos válidos para rediseñar esa cultura precedente a la que por siglos dominó el mundo: la de escritura. La cultura de la impresión, ("*The print cultura*" [6]), concomitante con la cultura del libro impreso, también llamada cultura del papel, hoy en día enfrenta un rediseño, tal como esta lo hiciera con la primigenia cultura del escrito, pues sus esquemas han quedado limitados en el tiempo, el espacio, forma y contenido frente al surgimiento de las nuevas tecnologías TIC.

Se estila que la cultura electrónica, ha producido varios cambios: unos, de tipo formal tras informar, o mejor dicho *comunicar* a los seres humanos en forma más interactiva y a velocidades electrónicas con textos, imágenes fijas o en movimiento, sonidos naturales o humanos, enlaces y vínculos dinámicos con otros tantos posibles textos a la vez situados en diferentes sitios del planeta. Toda esta diversidad en un solo cuerpo compuesto de páginas electrónicas interactivas e intercomunicables rápida y sencillamente por un comando del ordenador, con una o varias personas a la vez (*hipertexto*). Otras, de tipo técnico, porque *el espectro* electrónico global de las comunicaciones, a través de medios informáticos o electromagnéticos, en velocidades y formatos también electrónicas (binarias), sin distinción alguna ni límites geográfico,

---

(5) Resumiendo las argumentaciones del profesor Ethain, esta "nueva cultura", o mejor los impactos que ésta produce, se estructura, así: a) por las nuevas tecnologías de la información (TI), que no se llevan a cabo con 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 fronteras, a velocidades y formatos electrónicos; b) Por las capacidades que tienen los ordenadores o computadores mediante equipo idóneo para conectarse en red con cualquier parte de la tierra, posibilitando de esta forma la comunicación visual, auditiva y textual, a la vez. Estamos en el período de "surgimiento de las tecnologías" ("emerging technologies") que marcan nuevos derroteros y formas diferentes de regular la vida social, política, cultural, científica del hombre; y c) El trabajo investigativo en los diversos sectores sociales y las múltiples facultades que presentan los llamados hipertextos, entre las que están, la de extender las posibilidades de trabajo del ser humano con un grupo interactivo que maneje información que él necesita profundizar o complementar. KATSH, Ethain. *RIGHTS, CAMERA*.... Ob. cit., en el sitio de dirección internet *WWW. UMONTREAL.EDU.CA*. 1998.

(6) Ibídem, sitio y dirección internet, ut supra cit.

maneja las nuevas tecnologías TIC, el mundo de las redes de comunicación, como Internet y los aparatos y equipos computacionales (ordenadores: hardware y software) como un todo complementario para cumplir un único fin: potenciar la comunicación entre seres humanos, no deshumanizarla, ampliar los horizontes del conocimiento sin foraneidad alguna.

De esta forma se está creando nuevos espacios, que desafían abiertamente los actuales límites geográficos de los estados, que plantean nuevos modelos de autoridad dentro conceptos

diferentes a los que se tiene de la soberanía en los mapas y divisiones geopolíticas de hoy. Los nuevos mapas estatales y las relaciones virtuales o electrónicas entre las instituciones, organismos o entidades (sobre todo públicas) y las esferas de autoridades que trascienden los límites territoriales, representarán la escena del futuro de nuestras generaciones [7].

La Cultura electrónica de finales del siglo XX y principios del s. XXI, ha potenciado el manejo de la información activa y pasiva de tipo textual, visual o auditiva con tratamientos, procedimientos y formatos estrictamente electrónicos, a tal punto que hoy podemos hablar de una comunicación dinámica o electrónica que como surtidor genera una nueva visión de la vida personal, social, política, económica y científica. Aquí tan sólo abordamos un sector de la primera visión, y sobre todo, la que apunta a la llamada del *ciberespacio* [8] que emplea medios y aparatos electromagnéticos, ordenadores y las

---

(7) A estas conclusiones se llega, luego de analizar las "***Ways of Acting: New Relationships, Entities, and Institutions"*** pues, según Paul Saffo (En: *Business Goes Organic_The Acceleration of Technology Developments in 1995 Will Help Make Business More Like Biology*, Informationweek, Jan. 2, 1995, at 56.) has written that institutions are coming to be "defined by their relationships, not by their organizational boundaries.": What our experience with cyberspace reveals most clearly is that we are in an interconnected and overlapping set of spaces rather than a world where territory discretely and definitively separates sovereign states. Cyberspace, with its ability to move information across borders at electronic speed, will not replace either political entities or manufacturers of durable goods, though it does overlay a global communications network on top of a world that is and has been politically organized around territory and economically dependent upon the transportation of physical goods and resources. It does not necessarily cause old entities to vanish but it does change our experience with political and economic entities, our relationship with them, and the relationships between and among such entities". KATSH, Ethain. Ob. ut supra cit.,vía internet, 1998.

(8) El Ciberespacio es un término acuñado por el escritor de ciencia ficción William Gibson en 1984, cuando manifiesta: Cyberspace. Una alucinación colectiva experimentada diariamente por miles de millones de operadores de computadores en cada nación.... Una representación gráfica de los datos resumidos de los bancos de cada computador en los sistemas humanos. Una complejidad inconcebible. Un variado grupo de costelaciones de datos vuela sin espacio en la mente. Las ciudades se iluminan, recibiéndolos... (Neuromancer 51(1984). Cyberspace es todavía un término al que falta ser aceptado por todos en toda su significación. Aquí lo usamos como una propuesta en el camino de la maduración de una cultura electrónica, donde las redes electrónicas se generalice, se masifiquen, donde pueden comunicarse todo tipo de datos y estímulos instantáneamente alrededor del globo terrestre, y en donde los medios…" (Continúa página sgte).

tecnologías TIC para recoger, procesar y transmitir datos de carácter personal o familiar a través de redes globales (v.gr. Internet) o redes locales o sectoriales (v.gr. Intranet´s) y se destaca la nueva división del mundo entre quienes tienen acceso, almacenan o transmiten información, con medios TIC o no, a través del ciberespacio.

En las comunicación electrónica intranet´s los problemas no son exclusivamente transfronterizos, pero sí conllevan los ambientes de maleabilidad, dificultad y aspectos de tipo técnico y jurídico aún irresolutos del ciberespacio surcado por la red de redes de comunicación, como se le conoce a *internet*, en donde, por ejemplo, un investigador situado en la Biblioteca de la Universidad de Lleida (España), que disponga de un equipo electrónico idóneo, sin desplazarse físicamente de éste lugar, puede acceder, consultar y transferir datos de las

Bibliotecas Virtuales de Derecho, situadas en Montreal, Santa fé de Bogotá o Australia, compuestas de miles de textos y que serán miles de millones en tanto los enlaces y vínculos con otras tantas bibliotecas sean posibles, según las páginas electrónicas consultadas y los requerimientos del consultor, sin estar en el sitio, en el ambiente locativo, territorial y de tiempo real de aquéllas bibliotecas, y lo aparentemente más paradójico (que no lo es), sin haber abandonado Lleida y conseguido los fines investigativos imposibles de hacerlo en la cultura del papel impreso.

2. LA INFORMATICA Y LOS DATOS PERSONALES.

2.1. LA INFORMATICA JURIDICA o *IUSINFORMATICA.*

Iniciaremos con una conceptualización de la informática jurídica, luego haremos una breve sinopsis de la evolución de la *iusinformática* y finalizaremos con los impactos generados por aquella en las relaciones Estado-Individuo en la sociedad de la información o *informatizada*.

(Continuación de cita No. 8)
electrónicos a nuestra disposición aptos para adquirir y procesar información sean más ricos y más desarrollados de lo que son hoy. En el Cyberspace se incluye las herramientas que permiten que la información sea utilizada con las nuevas maneras y los elementos culturales de hoy en día, es decir, la cultura se orienta alrededor de información en forma digital en lugar de la información impreso. M. Ethain Katsh, Law in a Digital World 29 (1995); *see also* Dan L. Burk, *Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks*, 68 Tul. L. Rev. 1 (1993); Eric Schlachter, *Cyberspace, The Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, 16 Hastings Comm. & Ent. L.J. 87, 89 (1993); Edward J. Naughton, Note, *Is Cyberspace A Public Forum? Computer Bulletin Boards, Free Speech, and State Action*, 81 Geo. L.J. 409 (1992); Note, *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 Harv. L. Rev. 1062, 1087 (1994). En: *WWW.UMONTREAL.EDU.CA.*

Al conceptualizar a la informática jurídica, observábamos que esta tiene unos elementos constitutivos que le dan autonomía y un espacio en las ciencias jurídicas desde que el término *informática*, fuese acuñado por el francés *Philippe Dreyfus*, al analizar el tratamiento de la información realizado en la primera generación de los ordenadores o computadores (año 1955-1960) [8bis] , en la que se consideraron simples "máquinas automáticas" parecidas a las máquinas que realizan cálculos estrictamente matemáticos, aunque con evidente avance tecnológico, pues aquellas llevaban "*memo*- rias auxiliares" (v.gr. cintas electromagnéticas) y trabajaban con un programa de ordenador o software. De la unión de INFORMAción y automáTICA, nació el término, hoy generalizado: la *informática.*

Quizá por esto, *Davara* [9] y *Arus* [10], sostienen que la informática es la "ciencia del tratamiento automático de la información".

El iusinformático italiano *Frossini* [11], recogiendo el término de *Dreyfus* definió a la informática como la ciencia del "*traitement rationnel, notamment par machines automatiques, de I´information considerée comme le support des connsaissances et des communications dans les donmaines technique, economiques et social*" . Con esta _____

(8 bis) Las características y capacidades de los ordenadores o computadores, se han analizado según las "generaciones", por las que han tenido que atravesar desde que se presentaran a la opinión pública a mediados del presente siglo. Manuel LOPEZ MUÑIZ GOÑI (*INFORMATICA JURIDICA DOCUMENTAL*. Ed. Diaz de Santos S.A.Bilbao, (País Vasco), España, 1984.págs), destaca cinco generaciones: a) 1955-1960, b) 1960-1965, c) 1965-1972, d) 1972 en adelante, y e) En 1980. Japón toma la delantera con las innovaciones de alta tecnología aplicadas a los computadores. Aparece el concepto y contenido de "inteligencia artificial" o "prótesis artificial del cerebro humano", como la calificaba FROSINI. Esta inteligencia artificial es lo que pronto desarrollará la denominada "industria de la ingeniería del conocimiento". Estos ordenadores...van a poder analizar, informar, diagnosticar y hasta tomar decisiones en cuestiones relacionadas con elementos de producción y servicios, pero igualmente en otros temas de enorme importancia, como lo es el de los problemas de defensa... En el terreno científico, los ordenadores inteligentes van hacia el tratamiento automático de textos cualquiera sea la forma de esta escritos, la traducción automática... e incluso, la posibilidad de diálogo con la máquina en el propio idioma". Hoy algunas de estas facultades de los ordenadores (hardware) en unión indefectible e inseparable de los programas (software), han desarrollado estas y otras más funciones que superan a las de simple cálculo, conservación de la información, de encadenamiento lógico y de comunicación, capacidades con las cuales se conocieron a los computadores en los 80´s a los computadores.15 Citado en mi trabajo: ***La Constitución de 1991 y***... Ob. ut cit.pág. 51 y 130 y ss.

(9) DAVARA R. Miguel A. ***Manual de derecho informático***. Ed. Aranzadi, Pamplona (Esp), 1997, pag. 21.

(10) ARUS B. Francisco. ***El delito informático***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 11 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1994. Págs. 1 a 6.

(11) FROSINI, Vittorio. ***Informática y Derecho.*** Ed. Temis, Bogotá (Col), 1988, págs. 41-45.

definición, el autor adiciona un elemento importantísimo en la evolución de la informática y concomitante con la de los ordenadores. En la segunda generación (1960-1965), se mejora ostensiblemente la "memoria central" del com- putador, es decir, la unidad central de procesamiento de la información (CPU) y con aquél, el trabajo de acceso directo a toda clase de información con software y equipos idóneos se potencia rápidamente, se incorporan los "sistemas de trasmisión de datos" que constituyen la base de la intercomunicación de la información por medios eléctricos y electrónicos y los cuales se constituirían en el fundamento de las comunicaciones informáticas y telemáticas de hoy en día. La teletrasmisión de datos, la telegestión, el "time-sharing", etc; en fin, el mejoramiento de los equipos y aparatos computacionales, la miniaturización de los "chips"(microprocesadores de la información), el aumento de los unidades de almacenamiento de información (discos fijos o "duros" o flexibles o removibles, la familia de los Compac Disc, CD´s, etc), el perfeccionamiento de las unidades de acceso y salida de información ("unidades periféricas": monitores, impresoras, scaners, dispositivos ópticos: lápices, tableros, etc) y el software que soporta y complementa la labor lógica de almacenamiento, procesamiento y transferencia de la información, son subproductos de la tercera y cuarta generación de los ordenadores.

Ahora bien, la informática entendida como el conjunto de reglas, principios y procedimientos teórico-técnicos que incardinados estudian las formas de recolección, selección, organización, tratamiento, almacenamiento y transferencia (por cesión o consulta) de los datos o informaciones de toda clase, tipo, modalidad o fin, llevados a cabo por medios informáticos, electrónicos o telemáticos o por los que se llegaran a descubrir en el futuro, puede clasificarse según el tipo de información que se maneje. A nuestros propósitos, la endilgamos hacia las ciencias jurídicas. En tal virtud, la informática que maneja toda clase de información doctrinal, legislativa o jurisprudencial en el más amplio concepto del derecho, se le denomina *informática jurídica.*

La informática jurídica, en un sentido *lato*, estudia la información que se produce, procesa, almacena, transmite por medios informáticos, electrónicos y/o telemáticos en el derecho. El iusinformático español *López- Muñiz Goñi* [12], sostiene que la informática jurídica, tuvo como antecedentes; entre otros términos, la "jurimétrica", la "iuscibernética" y la "juritécnica", que por diferentes vías, ámbitos de

---

(12) LOPEZ MUÑIZ GOÑI, Manuel. *INFORMATICA JURIDICA DOCUMENTAL.*Ed. Díaz de Santos S.A. Bilbao, (País Vasco), España, 1984.págs. 15.

espacio y tiempo confluyeron a analizar y caracterizarla. En la actualidad, el fenómeno tecnológico de la información y la comunicación TIC y el derecho *ad portas* del siglo XXI, conforman un binomio que bien puede catalogarse de *ciberius o ciberderecho,* puesto que las autopistas de la información, la red de redes de la comunicación: locales (intranet´s) y globales (internet), la comunicación interactiva digital y el hipertexto constituyen una nueva lógica de asimilación y proceso de enseñanza-aprendizaje del derecho y la tecnología. Por ello, veamos, siquiera brevemente el antes y el hoy de este binomio.

En 1949, apareció el texto del abogado norteamericano *Lee Loevinger*, titulado: "*Jurimetrics: The next step forward*", en el cual explicaba que los adelantos tecnológicos iniciados con el computador conjuntamente con los programas para éstos, eran válidos en todas las ciencias humanas; y por supuesto, en el derecho. La Jurimétrica, entendida como la medida del derecho era factible como procedimiento lógico, racional y automatizada de la información jurídica, financiera y fiscal, y por ello, sus procedimientos para la época y lugar se validaron por entero.

En 1963, el Inglés *Hans Baade*, retoma la Jurimetría y aplica sus postulados al derecho consuetudinario anglosajón. Los Tribunales ingleses, comenzaron a aplicar la jurimetría como solución de las controversias ante ellos presentadas, tomando como medida del derecho los

"precedentes jurisprudenciales" catalogados y archivados coherentemente a través de mecanismos lógicos y matemáticos para establecer un banco de probabilidades soluciónicas al caso concreto.

En la práctica, la jurimétrica demostró inconsistencias puesto que los hechos sociales y jurídicos desfasaban las probabilidades preestablecidas, y sobre todo que los las controversias jurídicas no se podían someter a una regla o condición, prevista para las ciencias exactas, pero no las humanas, como el derecho, donde como se sabe, gran parte de las decisiones judiciales tiene un componente personalísimo o de subjetividad y otro normativo, basado en el Ordenamiento Jurídico o el precedente judicial. Sin embargo, se ha consideró este momento como la iniciación de lo que más tarde se llamaría *Vittorio Frossini* como la "prótesis de la inteligencia humana", aunque el sistema en sí mismo sólo sirvió para la historia de la informática jurídica.

El Juez Norteamericano *Wesley Hohfeld*, en sus providencias rebatió la jurimetría, manifestando que ésta ni es humana ni jurídicamente podía demostrarse su validez. Sin embargo, como enseña *Lopez-Muñiz Goñi* [13], no se trataba de demostrar que la Jurimétrica pudiera resolver las controversias jurídicas con una fórmula matemática mediante el computador sino de aplicar modelos lógicos a normas jurídicas y emplear la tecnología de la informática en las labores del jurista, del juzgador, el docente o el investigador de las ciencias jurídicas. Se trataba en últimas de poner en relación el "*ius con la cibernética*" y no de extraer una especie de “medida” para el derecho.

Surgieron concomitantemente con la anterior postura dos trabajos en donde se conjuntaba el derecho y la informática: El primero, el de *Mario Losano*, intitulado: La "Giuscibernética, in Nouvi sviuppi della sociología del diritto 1966-1967; y el segundo, el trabajo de *Vittorio Frosini*, titulado "Cibernética, diritto e Societá", 1968. Trabajos que produjeron debate jurídico, sociológico e incluso terminológico utilizado por la *iuscibernética* y sirvió para que conjuntamente con los avances tecnológicos de la información y la comunicación y el derecho, sean considerados en su justo sentido y con alcances y límites de los primeros hacia el último.

La *Juritécnica*, es un término acuñado por *Vittorio Frosini*, el cual abundó en la interrelación del derecho y las nuevas tecnologías y con alcances mayores a la jurimetría y a la iuscibernética, pues consideraba como principio fundamental la auxiliariedad de la informática frente al derecho y como un mero medio que está al servicio de éste.

Más recientemente, el profesor *López-Muñiz Goñi* [14], confirma expresamente el binomio: Informática-derecho (*Informática Jurídica o iusinformática*) y lo desarrolla amplia y profusamente en su obra citada, a tal punto que plantea las bases, métodos, procedimientos de entrada y recuperación de la información en el ámbito de la *informática jurídica documental,* aplicable al cúmulo de información producida por el poder público como la variadísima información que surge en las relaciones interpersonales o de éstas con los Estados, cuando el objeto principal del acceso, tratamiento, almacenamiento y transferencia de datos se concreta en *documentos* privados o públicos, generados por los particulares o por el Estado, en los diferentes negocios jurídicos y las diversas órbitas en que se aplican.

---

(13) Ibídem., pág. 16

(14) Ibídem., pág. 17

Hoy en día, tanto en el ámbito legislativo, doctrinal como jurisprudencial se produce una hiperexplosión de documentos jurídicos que llenan Bibliotecas Reales públicas y privadas en todos los Estados del mundo, por ello cada día con el advenimiento de las tecnologías TIC y el apoyo de la informática jurídica documental, hemos entrado en la era de las Bibliotecas Virtuales accesibles por medios informáticos, electrónicos o telemáticos desde cualquier parte de la tierra, sin límites fronterizos, ni obstáculos locativos, temporales ni espaciales por quien ubicado en un punto del planeta (una biblioteca real o desde propia casa, sin salir de ella) puede acceder, consultar y transferir información pertinente, oportuna, rápida y eficazmente. Podríamos decir, que nos hallamos ante el *ciberius o ciberderecho* porque la información jurídica se mueve por ese universo digital de las redes o autopistas de la información y comunicación. Los norteamericanos lo han llamado el *NetLaw* [15], puesto que el inmenso flujo de información o datos jurídicos que produce el Estado se transmite, emite y recepciona mediante la red de redes de comunicación, conocida como internet.

Las incidencias como los impactos jurídicas que brotan en relación con la información producida bien sean pública o privada y el poder de control y vigilancia del Estado, ejercido al acumular, organizar, manejar y autorizar el acceso, utilización y recuperación de la información por medios informáticos y electrónicos o telemáticos, tendremos oportunidad de puntualizarlo en la parte cuarta de este trabajo, cuando abordemos a la informática jurídica utilizada como mecanismo de control estatal o de intervencionismo en las relaciones sociales, políticas,

económicas, culturales, científicas, etc., con medios tecnológicos e incluso como medio de autocontrol de la información por parte del interesado [16].

En consecuencia, la informática jurídica surgida en los años sesenta hoy forma una nueva disciplina que con fundamento teórico, método y procedimientos propios se denomina *derecho informático,* y que *Davara* en España [17] y *Giraldo Angel* en

---

(15) Veáse, BARNES VASQUEZ, Javier. *La internet y el derecho. Una nota acerca de la libertad de expresión e información en el espacio cibernético. En:* Cuaderno de Derecho Judicial. C.G.P.J., Ordenación de las telecomunicaciones No.VI, Madrid, 1997, Pág. 241 y ss.

(16) Vid. mi trabajo: ***La Constitución*** .., ob ut supra cit., págs. 12 y ss.

(17) DAVARA R. Miguel . ***Manual*** ... ob. cit., pág. 25 y ss. Para comprobar la existencia de éste nuevo derecho, el autor vierte su contenido en los diferentes aspectos en los que se aplica la informática al derecho. A título enunciativo expone: la regulación de la "protección de datos", la "protección del software", "la contratación por medios electrónicos", "el delito informático", etc.

Colombia [18], lo han estudiado y caracterizado, para poder entender la insurgencia de las nuevas tecnologías TIC, en los diferentes campos del derecho en general, y el derecho público en particular. Uno de los aspectos que observaremos tras la óptica del
Ciberius o *NetLaw*, será el de los datos de carácter personal en la visión iusinformática de la intimidad.

2.2. LOS DATOS PERSONALES O DE CARACTER PERSONAL EN LA LEGISLACION COMUNITARIA, ESPAÑOLA Y AUSTRALIANA.

En la presente sección desglosaremos el concepto legislativo y doctrinal de "*datos de carácter personal"*, o simplemente: *"datos personales"*.

Una parcela de la informática jurídica se ocupa del estudio de los denominados *"datos personales"*, conceptualizados, regulados, categorizados y protegidos en las normas jurídicas comunitarias europeas (tales como, el Convenio de Estrasburgo del 28 de Enero de 1981 y ratificado en España por Instrumento de Enero 27 de 1984 [19] y la Directiva 95/46/CE del Parlamento y Consejo de Europa de 24 de Octubre de 1995 [20], principalmente) y los estatutos normativos especializados de cada Estado.

En España, los nominados "datos de carácter personal", constituyen un fenómeno jurídico sustantivo y procesal de derecho público que ha extendido su influencia tanto en el derecho administrativo como penal, por las implicaciones

---

(18) GIRALDO A., Jaime. ***Metodología y técnica de la investigación jurídica***. Ed.Profesional, Bogotá, 1985.

(19) El Preámbulo del Convenio Europeo de 19981, hace énfasis en los derechos fundamentales de información y la intimidad, cuando se refiere al "tratamiento automatizado" de los llamados "datos de carácter personal", su definición, clasificación, tratamiento y procedimientos y mecanismos para protegerlos . En efecto, sostiene: Que "Considerando que es deseable 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; Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; 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". Vid. AA.VV. *COLECCION DE DISCOS COMPACTOS: LEGISLACION ESPAÑOLA Y COMUNITARIA*. Ed. Aranzadi S.A., Pamplona, 1930-1998.

(20) 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"*. En los considerandos se destaca: "3.considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas; 4. Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos". Vid. AA.VV. *COLECCION.... Ob. cit.*

inherentes al ser humano, los impactos tecnológicos TIC y la evolución de la teoría de los derechos fundamentales y la *ciberius*. En efecto, para llegar a la conclusión actual de qué son los datos de carácter personal ha de tenerse en cuenta, entre otras normas, las siguientes: 1. Básicamente, la "*Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal" o* LORTAD (LO 5/1992, oct. 29) y sus numerosas normas de desarrollo v.gr. El Real Decreto de marzo 26 de 1993, por el cual se crea la "Agencia de Protección de Datos (APG)" [21], El Real Decreto 1332/1994, de 20 de Junio [22], La Resoluciones de Julio 18 de 1994 y de Febrero 7 de 1995, de la Dirección de la Agencia de Protección de Datos [23], la Instrucción 1/1995 de la Agencia de Protección de Datos, sobre información de solvencia patrimonial y crédito [24]; entre muchos otros. 2. Igualmente, en la creación de los numerosos

---

(21) El R.D. 26/3/93, Núm. 428/1993. Crea la Agencia de Protección de Datos en España. En un aparte del Texto de la norma jurídica se expresa: "El título VI de la Ley Orgánica 5/1992, de 29 de octubre, LORTAD, ha configurado la Agencia de Protección de Datos como el ente independiente que debe garantizar el cumpli-miento de las previsiones y mandatos en ella establecidos. Algunos aspectos de dicho ente han sido objeto de regulación en la propia Ley". Vid. AA.VV. *COLECCION..Ob. cit.*

(22) El R.D.1332/94, 20 de Junio, reglamenta el *derecho de habeas data*, particularmente sobre el derecho de acceso a la información (arts. 12 y 13), el derecho de rectificación y cancelación (art. 15). Igualmente, sobre los vías de tutela de los derechos reconocidos en la Constitución y la LORTAD, pues bien se sabe que actualmente existen varias vías y mecanismos jurídico-procesales para la defensa de los derechos contenidos en los datos personales, en vía administrativa y contencioso-administrativa. En la primera vía han sido objeto de reglamentación del mentado Real Decreto, la llamada "Reclamación en vía administrativa", ante la misma Agencia de Protección de Datos (APD), bien sea por reclamación o denuncia. Existen dos procedimientos: a) El procedimiento de tutela de derechos, previsto en el art. 17 de la LORTAD y 17 del Dec. 1332/94; y b) El procedimiento Sancionador (art. 47 LORTAD y 18 -19 R.D. 1332/94)

(23) Aquí debemos distinguir dos alternativas de información: 1. La Información sobre solvencia patrimonial y crédito de carácter positivo, es decir, que hace referencia a las posibilidades económicas y financieras de una persona física. Sólo podrán obtenerse los datos personales de esta clase de ficheros, en los siguientes casos: a) de fuentes accesibles al público, provenientes de ficheros de titularidad privada, b) de informaciones facilitadas por el afectado, c) de cesiones consentidas por el afectado. 2. Ficheros cuya finalidad es el almacenamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias. Sólo podrán obtenerse los datos personales de esta clase de ficheros del acreedor, o de quien actúe por su cuenta o interés.

(24) 1. La Resolución de Julio 18 de 1994. Regula los ficheros automatizados de datos de carácter personal existentes en la Agencia de protección de datos. La disposición adicional segunda, número 2, de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), establece que dentro del año siguiente a la entrada en vigor de dicha Ley Orgánica, las Administraciones Públicas responsables de ficheros automatizados ya existentes deberán adoptar una disposición de regulación del fichero, o adaptar la que existiera. Por otra parte, el Real Decreto-ley 20/1993, de 22 diciembre, prorrogó por seis meses el plazo de un año al que se ha hecho referencia. En el ejercicio de las atribuciones que me confiere el artículo 22.2 de la Ley Orgánica 5/1992, y a fin de dar cumplimiento al mandato legal de adecuación de los ficheros automatizados gestionados por la Agencia de Protección de Datos y asegurar a los administrados el ejercicio de sus legítimos derechos. 2. La Resolución de Febrero 7 de 1995. Crea ficheros automatizados de datos de carácter personal en la Agencia. El artículo 18 LORTAD, establece que la creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o en el "Diario Oficial" correspondiente Vid. AA.VV. *COLECCION*.. ut supra cit.

"ficheros de titularidad pública y privada", posibilitados por los arts. 18 y 23 LORTAD, respectivamente [25]; en las normas jurídicas de las Comunidades Autónomas, referidas al tema, como la Madrileña de 1995 [26], y 3. finalmente, las normas jurídicas especiales [27] excluidas del régimen jurídico de la LORTAD.

---

(25) A título de ejemplo: 1. Banco de España: Resolución 13/6/97, por el cual se "Hace públicos los ficheros con datos de carácter personal bajo responsabilidad de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias gestionados por el Servicio Ejecutivo de la misma". 2. Ficheros de las diversas universidades españolas. v.gr. a) Rectorado de Universidad de Granada: Resolución 31/3/97. Regula los ficheros de tratamiento automatizado de datos de carácter personal de la Universidad, b) Univ. Alcalá de Henares:Resolución: 27/7/94. 3. Los diferentes ficheros de los Ministerios del Estado. v.gr.: a) Ministerio de la Presidencia: Orden 14/3/93. b) Ministerio de Justicia e Interior: Orden 26/7/97 (La Orden de Junio 28 de 1995. Crea el fichero automatizado Base de Datos de Señalamientos Nacionales (BDSN) gestionado por el Gabinete de Coordinación de la Secretaría de Estado de Interior). c). Ministerio de Educación y Ciencia: Orden 26/7/97 d) Ministerio de Trabajo y Asuntos Sociales: Orden 26/10/96 y e) Ministerio para las Administraciones Públicas. El Real Decreto Núm.263 de Febrero 16 de 1996. Regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

(26) Ley 21-4-95, Núm. 12/1995. Regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid. En el Texto de la Ley se destaca inicialmente, algunas argumentaciones ciertamente controvertibles, al sostener: " Si pueden admitirse excepciones a la regla general que predica el desfase de las normas de derecho positivo respecto de las manifestaciones de la realidad social que regulan, estamos frente a una de ellas, y no tanto porque la materia objeto de regulación, la aplicación de la informática al tratamiento de los datos personales por la Comunidad de Madrid, sea un fenómeno reciente, que a este respecto se cumple la regla general, como por la ausencia de una demanda social de legislación en relación a la materia. En efecto, los fenómenos que en esta ocasión aconsejan legislar ocupan en la escala de las preocupaciones de la sociedad un bajísimo lugar: la amenaza que objetivamente constituyen las tecnologías de la información y, particularmente, la informática para la privacidad de los ciudadanos no origina más que un estado de indiferencia social sólo quebrado ocasionalmente por noticias de tráfico de información de carácter personal, presentadas de modo alarmista y orwelliano, que abandonan rápidamente la cabecera de la actualidad. Los expertos y profesionales de estas técnicas de tratamiento de la información, conscientes, por el propio ejercicio de su oficio, de los riesgos en presencia, son precisamente quienes han estado en el origen de la denuncia de los problemas derivados de la aplicación de las tecnologías de la información a los datos de carácter personal y de la exigencia de un sistema de límites a la utilización de las mismas. Nacida de este segundo movimiento, es la presente, en ese sentido, una Ley ilustrada, uno de cuyos valores esenciales debe precisamente buscarse en su contribución a promover un adecuado nivel de información y conciencia social sobre la amenaza, en absoluto de ficción científica, a la que se ha hecho mención. " Vid. AA.VV. *COLECCION DE DISCOS*... ut supra cit.

(27) Regímenes especiales sobre "tratamiento automatizado" de datos de carácter personal, regidos por "leyes especiales" y no por la LORTAD (art.2.3), pero que llevan inmerso el concepto de datos personales. Los principales son: 1. En el Régimen electoral: a) Ley Orgánica 5/85 de 19 de junio ; b) Ley Orgánica 13/94 de 30 de marzo, que modifica a la anterior. 2. En "Materias clasificadas": (secretos oficiales): a) Ley 9/68 de 5 de abril; b) Ley 48/78 de 7 de octubre que modifica a la anterior. 3.

En el Registro Civil: a) Ley de 8 de junio de 1957, b) Reglamento del Registro Civil, Decreto de 14 de noviembre de 1958. 4. En el Registro Central de Penados y Rebeldes 5. En Los datos que sirvan exclusivamente para fines estadísticos amparados por la ley 12/89 de 9 de mayo de la Función Estadística Pública. 6. Los informes personales a que se refiere el artículo 68 de la Ley 17/89 de 19 de julio del régimen del personal militar profesional.

En consecuencia, se hace referencia a los *datos de carácter particular o datos personales*, (se excluyen los datos de las personas jurídicas, al menos del ámbito jurídico comunitario y español [28]), para designar a toda clase de información (textual, auditiva, de imágenes, o video auditivas) relativa a las personas naturales o físicas (identificada o identificable) o *concernidas* que son objeto de recolección, registro, tratamiento, almacenamiento y trasmisión (cesión, consulta y flujo transfronterizo) por medios informáticos, electrónicos o telemáticos [29] y cuya conceptualización, principios que los gobiernan, clasificación o categorización, mecanismos y procedimientos jurídicos que sirven para su tutela en vía administrativa, contencioso-administrativa y jurisdiccional (constitucional y penal, básicamente), se hallan previstos en el ordenamiento jurídico vigente.

Las expresiones "*cualquier información*", utilizados por la LORTAD en el art. 3-a, para conceptualizar los datos concernientes a una persona, deben interpretarse en términos iusinformáticos como una unidad de datos (sea textual, gráfica, imágenes fijas o móviles, auditivas o vídeo-auditivas) representada en forma binaria (ceros y unos) en el tratamiento electromagnético o computarizado (especialmente en su almacenamiento --storage-- y teletrasmisión en unidas compatibles de discos fijos o "duros", de discos de acetato o "flexibles", o de discos compactos "Compac Disc" o medios informáticos de software o hardware, respectivamente) y relacionada con una persona natural o física. La información recolectada, seleccionada, organizada, procesada, almacenada y recuperada mediante consulta o transferencia, total o parcialmente por medios no simplemente "automatizados", sino por dispositivos o aparatos eléctricos, electrónicos o electromagnéticos (telecomunicaciones y ordenadores, básicamente). Todo ello, obviamente de contextualizarse en las consideraciones de que esa "cualquier información", está dentro del marco constitucional de derechos y libertades inherentes

---

(28) Como también lo reconoce el profesor Orti Vallejo, el art. 1 de la LORTAD, siguiendo el criterio dominante --aunque no unívoco-- de las leyes de protección de datos extranjeros (EE.UU, Alemania, Francia), deja fue-ra del marco protector de la misma los datos relativos a la personas jurídicas. Sin embargo, esto no implica que las personas jurídicas queden desprotegidas, pues el "prestigio o el secreto de los datos de las personas jurídicas constitucionalmente", están cubiertos con garantías civiles como la del art. 1092 C.c, entre otras posibilidades, como las garantías de protección de carácter penal a las que nos referiremos en la IV de este trabajo. Vease, ORTI VALLEJO, Antonio.*DERECHO A LA INTIMIDAD E INFORMATICA (Tutela de la*

persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada). Ed. Comares, Peligros (Granada), Esp., 1994, pág. 74 a 79

(29) En la parte IV, puntos 5.2.5., 5.2.5.1 a 5.2.5.3., profundizaremos sobre los medios informáticos, electrónicos o telemáticos, sus impactos en la sociedad de la información y la descripción y clasificación de los mismos, según pertenezcan al llamado hardware o equipos y aparatos computacionales, o a los programas de computador o software

a la persona humana (arts. 14,15,16 y 55.1 CE), los valores y principios, tales como la dignidad, el desarrollo de la personalidad, el interés público, la paz social y democrática (art. 10 CE); y por su puesto en los límites constitucionales de los derechos de los demás previstos en la propia constitución (arts. 18.4 y 20.1 CE) y la LORTAD y demás normas de desarrollo. De lo contrario, el término "cualquier" vaciaría de contenido a la ley, por lo ambigua, amplia, sin límites formales o de contenido y sin esquemas de protección jurídica sustantiva o procesal que le quepa.

Igualmente, será *"persona identificable"*, a quien le concierne cualquier información (LORTAD, ibídem), según la Directiva 95/46/CE, *"aquella a quien puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social* (art. 2.a.).

En igual sentido la *Privacy and data Protection Bill 1994 (NSW) Australiana*, art. 3 **[30]**, define a la información personal como la información u opinión (incluida la que hace parte de un banco de datos), verdadera o no, registrada en un forma material o no, sobre una persona cuya identidad esta plenamente determinada o se puede determinar razonablemente.

De esta última definición destaquemos la forma en que debe ser registrada la información (esta incluye la recolección, selección, organización y almacenamiento), pues se hace alusión a las formas materiales o no. En efecto, la Ley de protección de la intimidad contenida en los datos de 1994 Australiana, expresa que el registro de la información puede hacerse en un documento (*Act 1987* Australiana, extiende el concepto a la información que se halle en discos, cintas u otro medio que registre sonidos, imágenes o mensajes capaces de ser reproducidos), o en una fotografía o representación pictórica de una persona, que no incluye a las que aparecen en revistas, libros, periódicos u otras formas de publicación disponibles al público o se encuentre en un archivo estatal (Según el *Act 1960*, sobre Archivos Australiana), en una biblioteca, galería de arte o museo, con propósitos de referencia, estudio, exhibición o sean objeto de trasmisión por carta o cualquier mecanismo de correo.

---

(30) *Privacy and data Protection Bill 1994 (NSW) Australiana*. Texto completo en *WWW.AUSTLLI.EDU.AU*. Biblioteca Virtual de Derecho de la Universidad de Australia -- Austlli--. Vía Internet, 1998.

Un aspecto capital que va incardinado con la conceptualización de los datos de carácter personal, es el atinente a los principios de protección establecidos tanto por las Leyes Comunitarias Europeas como por la LORTAD Española [31] e incluso por la Ley de protección de los datos y la intimidad Australiana .

En efecto, en la *Privacy and data Protection.* Bill 1994 (NSW), como norma específica de protección de la visión iusinformática de la intimidad, en la Parte 2, sobre Vigilancia y protección de los datos, División 4, sobre los principios de protección de los datos (art. 21), los enuncia así: a) Manera y propósitos de la recolección de información, b) Solicitud de información por parte del individuo concernido o involucrado, c) Solicitud de información general o de dominio público, d) Almacenamiento y seguridad de la información, e) Información relativa a los datos registrados ante una autoridad competente, f) Acceso a los datos que contienen información personal, g) Alteración de los datos registrados que contienen información de las personas, h) Verificación de la exactitud de los datos que contienen información personal antes de ser utilizados, i) Límites al uso de la información personal, j) Límites en el descubrimiento o divulgación de la información personal, y k) Límites al uso de cierta información, tal como los que revelen el origen racial o étnico, opiniones políticas, creencias religiosas, salud o vida sexual. Igualmente, los límites al uso de información sobre la historia delictiva de las personas. En estos últimos casos, sólo se procederá por la autoridad competente, persona autorizada o responsable de un banco de datos, previo consentimiento expreso, escrito y libre otorgado por el concernido o cuando la ley lo autorice, o mediante el establecimiento de un código de protección de datos, respectivamente.

---

(31) Los principios de protección de los datos personales se hallan inmersos en el Título II, arts. 4 a 11 LORTAD, bajo las siguientes rúbricas: a) Calidad de los datos, b) Derecho de información en la recogida de datos, c) Consentimiento del afectado, d) Datos especialmente protegidos, e) Datos relativos a la salud, f) Deber de secreto y g) Cesión de datos. Como veremos la técnica utilizada por el legislador español, en éste aspecto, tiene serios reparos, pues juntamente con los principios se regulan los derechos y obligaciones de los sujetos titulares del procedimiento de regulación de datos por medios informáticos, electrónicos y telemáticos. El Convenio Europeo de 191, prevé los principios bajo los siguientes epígrafes: a) Calidad de datos (art.5) y b) Categorías especiales de datos (art.6). Aquí se destaca la prohibición de todo procedimiento de tratamiento de datos relativos al origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos relativos a la salud, a la vida sexual o los referentes a las condenas penales. En la Directiva 95/46/CE, de 24 de Octubre, prevé los principios de protección de los datos bajo los intitulados siguientes: a) Principios relativos a la calidad de los datos, y b) Principios relativos a la legitimación del tratamiento de datos (arts.6 y 7).

La importancia capital del estudio de los principios de protección de los datos, a nuestros efectos, se centrará en todo el procedimiento de regulación de los datos personales por medios

informáticos, electrónicos o telemáticos, tal como implícitamente se describe en la exposición de motivos de la LORTAD, al decir:

> *Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandado constitucional, se pretende limitar.*

Por estas razones, al final de este parte del trabajo abordaremos este tema de tal forma que sean analizados los principios de protección de los datos, a través de las fases inicial o "*input*" de datos, de tratamiento propiamente dicho o "*in*" de datos y la fase salida o "*output*" de datos dentro de la visión iusinformática de la intimidad que involucra los derechos de *habeas data,* intimidad e información --*The Right to control information about oneself* (del Common Law americano) y el de oposición al tratamiento informatizado de datos personales (del Derecho Comunitario Europeo)--.

La categorización de los datos personales, los niveles de protección jurídica sustantiva y procesal, planteada por el art. 6 del Convenio Europeo de 19981, ratificada en la LORTAD y la Directiva 95/46/CE, art. 8 y ss., será abordada en la Parte IV, de este trabajo [32], cuando no dediquemos a tratar los denominados "datos sensibles" de la persona humana, a los diferentes grados de protección de los datos o informaciones personales del concernido, titular o interesado (que no "afectado" como impropiamente utiliza este término la LORTAD y sus normas de desarrollo), así como la protección penal que la legislación penal española prodiga a los datos sensibles, hipersensibles y ultrasensibles.

2.3. LA INFORMATICA JURIDICA DOCUMENTAL Y LOS "BANCOS DE INFORMACION PERSONAL".

Analizaremos la necesidad recíproca de la informática jurídica documental y el

---

(32) Véase, Parte IV, puntos 5.2.3, 5.2.3.1 a 5.2.3.3.

derecho, la espina dorsal de la misma: *el Thesaurus*, para terminar con una introducción al estudio de los sistemas de tratamiento de la información por medios informáticos y correlativamente la de los denominados bancos de información personal (*personal information bank.*).

La informática jurídica, según el iusinformático español *López Muñiz-Goni* [33], se divide, así: a) Informática jurídica operacional, la cual se dedica a la gestión de los juzgados, Bufetes profesionales, Cámaras legislativas, etc., b) lnformática Registral destinada a procesar, almacenar y registrar todos los documentos públicos o privados en los cuales sea necesaria dicha actividad, c) Informática jurídica decisional, por medio de la cual se "llega a la resolución automática de los casos, a través de ordenadores electrónicos que manejan la llamada ´inteligencia artificial´y conocidos por otros como ´prótesis de la inteligencia humana´"; y d) Informática jurídica documental o documentaria, relacionada con los bancos de datos jurídicos en lenguaje natural, destinados principalmente al manejo de los datos o informaciones atinentes a la legislación, la jurisprudencia, doctrinales, bibliográficos o materias jurídico sociales especializadas que reúnan datos conexos, organizados, clasificados y puestos a un servicio o fines igualmente específicos y determinados. Esta última clasificación de la informática es la que nos sirve de fundamento para el presente temario.

La informática jurídica documental, opera en base al lenguaje documentario elaborado a partir del lenguaje jurídico, compuesto por palabras claves y descriptores extraídas de éste y ulteriormente clasificadas e insertadas en la estructura lógica de un ´thesaurus jurídico´, según sostiene *Castells Arteche* [34].

El Thesaurus (Thesauro o tesoro de palabras), proviene del griego que significa aglomeración, almacenamiento, compilación o acumulación. Según *Van Dijk,*

> *El Thesaurus puede ser definido como una lista de términos normalizados y convencionales, que forman un lenguaje documental. Cada término representa un campo semántico que rebasa generalmente la definición que da el diccionario y un campo documental acompañado de sinónimos, cuasi-sinónimos y palabras relacionadas, así como cuantas otras relaciones se estimen oportunas entre campos vecinos...* [35].

---

(33) LOPEZ MUÑIZ-GONI, Manuel. *INFORMATICA JURIDICA DOCUMENTAL.* Ed. Díaz de Santos. S.A., Bilbao, España, 1984, págs. 15 y ss.

(34) CASTELLS ARTECHE, José Manuel. *LA LIMITACION INFORMATICA.* En: Estudios sobre la Constitución Española. Estudio Homenaje al profesor Eduardo García de Enterria. Ed. Civitas, Tomo II, Madrid, 1991, pág. 911

(35) Citado en mi libro *LA INFORMATICA JURIDICA... O*b.ut supra cit. pág. 73 y ss

Hoy, *ad portas* del nuevo milenio, navegamos en una sociedad donde nuestras actividades sociales, culturales, políticas, jurídicas, económicas o financieras e incluso las catalogadas de carácter personal, constituyen el fundamento de *cualquier información* o la esencia de los *datos personales o familiares* susceptibles de ser recogidos, tratados, almacenados o transmitidos por medios mecánicos, eléctricos o electromagnéticos (o telemáticos). Valga retomar, el simil inicial sobre la producción hiperexplosiva de información o datos personales y/o familiares (de todo tipo: textual, auditivo, gráfico, video-auditivo o de caracteres alfanuméricos) y el origen, desarrollo, muerte y efectos post morten de un ser humano, para demostrar que hoy todavía navegamos en una cultura de la escritura, seguida de la cultura del impreso y que apenas sí hemos dado un paso firme en vías a esa cultura que el profesor *Ethain,* denomina la *cultura electrónica,* cuando comprendemos los volúmenes inconmensurables de información contenida en papeles, cartas, escritos, imágenes, gráficos, y sobre todo, documentos (públicos o privados) y a la vez, empleamos nuevos medios (los de la tecnología TIC y la informática) para crear, procesar o transferirla muy distintos a los tradicionales (escritura y/o impresión), a fin de facilitar, ampliar el volumen y la calidad, como también disfrutar las nuevas alternativas de manejo audiovisual y sensitivo en el estudio, consulta, investigación o simplemente la curiosidad de leer y contestar un misiva institucional, empresarial o personal.

Precisamente para paliar algunas de las más sentidas dificultades de la cultura de la impresión y consecuente reforzar la cultura electrónica en todo lo atinente a la recolección, selección, organización, tratamiento y transferencia (cesión o consulta) de datos o informaciones, se han introducido mecanismos, elementos, aparatos y equipos eléctricos y electrónicos, que comienzan a masificarse a partir de la década de 1980 en todo el mundo. A título de ejemplo, citemos los llamados por el iusinformático español *López Muñiz-Goñi* [36], *sistemas de tratamiento informatizados* viabilizados a través de medios informáticos, electrónicos o telemáticos de carácter material o de hardware o de carácter intangible, lógico o de software (conocidos como programas de computador).

Los sistemas de tratamiento informatizado, entendiendo por tales, "*aquellos de carácter informático utilizados para establecer los criterios de búsqueda de los documentos*"[37], previa recogida, selección, organización, estructuración, almacena-

---

(36) Ibídem., pág. 71
(37) Ibídem., pág. 71

miento y registro, a través de medios informáticos, electrónicos o telemáticos. En consecuencia, estos sistemas de tratamiento informatizado apuntan a dos extremos bien definidos: los sistemas de entrada y salida de la información.

Hoy en día, se conocen dos sistemas de entrada o acceso (*input*) de la información : a) El sistema de texto completo o "*full text*", y b) El sistema de descriptores (o de thesaurus). En tanto, que los sistemas de salida o recuperación (*output*) de información, actualmente son: a) Sistema referencial, dividido a su vez en: sistema de pura referencia y sistema de referencia documentada, b) Sistema de resúmenes, y c) Sistema de texto completo. En la sección final de este parte del trabajo ampliaremos lo pertinente sobre el tema.

Ahora bien: estos sistemas de acceso, almacenamiento y recuperación de información o datos de cualquier especie o clase, estructurados en forma lógica, a través de procedimientos y medios informáticos, electrónicos o telemáticos, con soportes, elementos, aparatos y equipos de carácter material o de *hardware* (ordenadores: con unidades centrales de procesamiento --CPU-- y periféricas v.gr. monitor, impresora, modem, etc) o de carácter intangible, logiciales o de *software* (programas de computador), constituyen el fundamento técnico y lógico de lo que se conoce como bancos, bases o "ficheros" de información personal o también conocidos como "Bancos de Datos" (*Bank of date o "database"*). Según el tipo de información o datos que se maneje tomarán los subnombres de Banco de datos jurídico, documentario, financiero o económica, etc. Los bancos de datos jurídicos, a su vez , pueden ser: jurisprudenciales, doctrinales, legislativos o parlamentarios, de las administraciones públicas, etc.

El Banco de Datos es una estructura lógica de acceso, almacenamiento y recuperación de información, y por tanto, no puede ser sólo un simple "*depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones*" [38], puesto que disponen de un lenguaje propio construido para lograr la identidad literal o conceptual entre el vocabulario utilizado por el usuario de un banco de datos, y del documento que pretende consultar (la estructuración de un thesaurus). Esto pone de manifiesto la magnitud de la tarea que se pretende emprender para elaborarlo, y su complejidad, pero a la vez pone de relieve su importancia. Podemos afirmar sin lugar a dudas que de la adecuada construcción del thesauro depende en gran medida la eficacia de un banco de datos de carácter documental [39].

---

(38) DAVARA R. Angel. *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi, Pamplona, 1997, pág. 133.
(39) GIRALDO ANGEL, Jaime. *INFORMATICA JURIDICA DOCUMENTAL*. Ed. Temis, Santa fe de Bogotá, 1990, pág. 10

La incorporación de los bancos de datos en el mundo de la reglamentación jurídica es relativamente reciente. Las textos normativos en los Estados comienzan a referirse a ellos, desde diferentes vertientes: unas veces para reglamentarlos los derechos de autoría de las

obras intelectivas conocidas como “bases de datos”, tanto en la creación, aplicación, clases y mecanismos jurídicos sustantivos y procesales de protección [40]; otras, para poner de manifiesto “el desconocimiento de esta realidad (impacto de las tecnologías TIC y las bases de datos) podría llegar a producir una sensible merma de diligencia en el ejercicio de sus actividades habituales pudiendo en ciertos casos, llegar a provocar la interposición de las correspondientes acciones civiles o penales por negligencia profesional, dado el actual ´estado de la ciencia´, cuyo conocimiento se exige a dichos cualificados profesionales”[41], o finalmente evidenciar la potencialidad del riesgo como el nivel de protección tecnológicos de los derechos, libertades públicas e intereses legítimos contenidos y continentes en una banco de datos. En efecto, “los ficheros” o bancos como estructuras lógicas de acceso, almacenamiento y recuperación de la información a través de procedimientos y medios informáticos, electrónicos o telemáticos, utilizadas en el manejo, administración y control datos de carácter personal, por autoridades, personas o responsables de un banco, base o fichero, trátense de titularidad pública o privada y de contenidos permitidos y autorizados por el ordenamiento jurídico v.gr. LORTAD en España, la *Privacy and data protection Bill 1994* (NSW) en Australia. A éste última especie de Bancos de Información Personal o Banco de Datos nos referimos en el presente trabajo.

---

(40) DAVARA R. Angel. *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi, Pamplona, 1997, pág. 133 y ss.

(41) El mercado de las bases de datos, consolidado a finales de la década de 1950 en los Estados Unidos y a finales de la década de 1960 en Europa, ha venido manteniendo un crecimiento continuado en la producción de bases de datos on-line que supera, en la actualidad, las 8500 unidades operativas que almace-nan más de 6000 millones de registros, estando auspiciado dicho crecimiento, en el sector de las ciencias jurídicas,por el apoyo suministrado por las diferentes Administraciones públicas, órganos jurisdiccionales, parlamentos, universidades, colegios profesionales, instituciones de investigación, etc., ligadas al desarrollo de las ciencias sociales. En este mercado, las bases de datos jurídicas constituyen cerca del 20% de la oferta total de las bases de datos, lo que pone de manifiesto el interés institucional y social sobre las mismas, generado por dos imperiosas necesidades, la de modernizar la gestión judicial evitando retrasos injustificados en los diferentes procesos y la de reducir la inseguridad jurídica provocada por la cada vez más compleja composición y estructuración de los diferentes ordenamientos jurídicos, promoviendo su conocimiento por medios útiles informáticos especialmente diseñados para ello. Vid. PAEZ PEÑA, Jorge. *COMENTARIOS SOBRE ALGUNAS PARTICULARIDADES DE LAS BASES DE DATOS JURIDICAS.* En: Revista Actualidad Informática Aranzadi, Ed. Aranzadi, S.A., Núm. 16 de Julio, Pamplona, 1995, págs. 1-4 y ss.

2.4. LOS DATOS DE CARÁCTER PERSONAL EN SOPORTES Y/O MEDIOS INFORMÁTICOS, ELECTRÓNICOS O TELEMÁTICOS

Las normas comunitarias europeas y las españolas, a partir de la década de 1980, comenzaron a introducir un lenguaje tecnológico antes no visto, debido principalmente a los

avances de las ciencias de la información y la comunicación y al surgimiento de una compleja costelación de elementos, soportes, aparatos y equipos que estas empleaban; y por supuesto, a la necesidad de las ciencias jurídicas de recoger una terminología que resulte acorde con la novísima tecnología y se refleje en las normas reglamentarias que cada Estado produce y logre así, armonizar el conocimiento humano, la tecnología y el derecho.

Las normas jurídicas comenzaron entonces, a incluir en las exposiciones de motivos, preámbulos, parte preliminar e incluso en los artículos iniciales unas definiciones técnicas, muchas veces cerradas, complejas e ininteligibles pero estrictamente necesarias para el entendimiento global del objeto reglamentado en dicha norma jurídica. Algunas normas son básicamente un thesauro bien estructurado de definiciones donde el operador jurídico poco o nada puede aportar, pues manejan un lenguaje altamente tecnológico de no fácil inteligibilidad si se toma por separado los conceptos explícitos en esta, o más aún, no se estudia su enclave, vinculación o remisión a otras normas donde se amplia el concepto, se retoma la definición o se explica en una magnitud que es imposible hacerlo en la definición inicial. Este es el caso del Código Penal Español que utiliza los conceptos: "fichero", "soportes informático, electrónico o telemático", "archivo", "registro", "telecomunicación", "programas de computador", etc., o el caso parcialmente de la LORTAD. LO.5/1992, Oct.29, que incluye algunas definiciones de "Datos de carácter personal", "fichero automatizado", "tratamiento de datos", etc, o la Ley de Régimen jurídico de las Administraciones Públicas y procedimiento administrativo común. LRJPA. Ley 30/1992, Nov. 26, hace referencia a "Documento...informático, electrónico, telemático". Por ello, para sólo referirnos aquí a los soportes y medios informáticos, electrónicos o telemáticos, acudiremos a éstos dos últimos textos y a otros que nos explican qué debemos entender por tales, a efectos del derecho.

2.4.1. EL "SOPORTE" INFORMATICO EN EL DERECHO.

Precisaremos el concepto de soporte informático y describiremos su clasificación.

El R.D. 263/1996, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración del Estado, al reglamentar principalmente el art. 45 de la LRPJA, sostiene: *Soporte es el objeto sobre el cual o en el cual es posible grabar y recuperar* información o datos de cualquier tipo (art.3. a),). Desde el punto de vista de la informática, el soporte constituye el dispositivo idóneo en el cual se puede acceder o entrar (input), almacenar, procesar y recuperar (output) información análoga o digitalizada (textual, gráfica, imágenes, video-auditivas en forma binaria "ceros y unos" 0-1). v.gr. los discos magnéticos no removibles o fijos o "hard Disk" (discos mal llamados *duros*, por la traducción literal que no encierra un

significado asimilable en nuestra lengua) y la variopinta clasificación de los discos flexibles o removibles: a) discos de acetato: Discos de 3 □ y 5 1/4 pulgadas, b) la familia de los discos compactos (*Compac Disc*) que aumentó ostensiblemente la capacidad, la versatilidad del disco de acetato y potenció el almacenamiento y recuperación de información de texto, gráfica, auditiva y visual. Entre los más importantes, están: El típico CD, CD-ROM --sólo lectura--, CD-RAM -- lecto- escritura-- CD-I -- audio, video e interactivo y el DVD --Disco Digital de Vídeo o Disco digital versátil-- que supera en siete veces la capacidad de su predecesor CD, y c) Los denominados "Backups" o unidades de cinta, estilo cassette, para copias de seguridad en un sistema de procesamiento de datos de cualquier tipo, corrientemente utilizados en el sector comercial y financiero, privado y público, para salvaguardar grandes cantidades de información o datos, almacenados y organizados en forma diaria, mensual o anualmente o por sistemas de ordenación utilizados en la estadística o las ciencias matemáticas o sociales.

Los soportes, entonces, son los elementos o dispositivos materiales conocidos o conocibles sobre los cuales se puede ingresar, almacenar y recuperar información o datos de cualquier tipo o clase. Son elementos continentes de información estructurada lógica e informáticamente. Por ello, los soportes en este sentido se denominan informáticos y dependiendo si sólo dentro de ellos se ingresa y almacena información se denominarán informáticos, pero si además de aquello, son objeto material e imprescindible de trasmisión de los mismos, por medio de las tecnologías de la información y la comunicación (TIC) y otros equipos y aparatos electromagnéticos como un ordenador y un *Modem*, se denominarán soportes *electrónicos y/o telemáticos.*

En consecuencia, los *soportes informáticos o electrónicos*, como dispositivos materiales de variada forma, con complementarias funciones y con iguales sistemas de estructura lógica de almacenamiento de información (forma binaria), son continentes de información o datos generales o específicos básicamente en discos electromagnéticos removibles o flexibles (como los "disquetes"), en cintas de backup (almacenan grandes cantidades de datos o informaciones como "copias de seguridad" de un usuario), discos fijos o removibles y los discos compactos (CD´s), en los cuales el mensaje se consigna mediante *magnitudes físicas que representan en forma codificada unas nociones o noticias y son susceptibles de registro, proceso y trasmisión* [42].

2.4.2. EL "MEDIO" INFORMATICO EN EL DERECHO. El "HARDWARE" Y EL "SOFTWARE" [43].

Ahondaremos sobre lo que en derecho debemos entender por "*medio*", o mejor medios, pues describiremos los medios físicos, materiales o de "hardware", los medios inmateriales, intangibles o de "software", como también los medios provenientes de las nuevas tecnologías de la información o comunicación (TIC). Todos ellos constituyen lo que denominamos *medios informáticos, electrónicos o telemáticos.*

Ahora bien, entendemos por "*Medio*", *el mecanismo, la instalación, el equipo o los sistemas de tratamiento de la información que permite, utilizando técnicas electrónicas, informáticas o telemáticas, producir, almacenar o transmitir documentos, datos e informaciones*. (art.3, b), R.D. 263/1996, 16 de Febrero). En este sentido el soporte es un medio que cumple algunas de las funciones complejas de éstos, como pueden ser el almacenamiento y trasmisión de datos, pero obviamente no todas ni mucho menos que los suplante.

En términos iusinformáticos, se consideran medios, los de carácter físico, materiales o denominados también *Hardware*. Se consideran tales: 1. El Ordenador o Computador, compuesto de varias partes eléctricas y electrónicas dentro de las que se destacan: a) El procesador continente de la Unidad Central de procesamiento de la información o --CPU--; b) La memoria o ambiente de trabajo del propio ordenador; c) Las unidades de entrada y salida (E/S) de información; d) El almacenamiento en disco

---

(42) Vid. HEREDERO HIGUERAS, M. *VALOR PROBATORIO DE LOS DOCUMENTOS ELECTRONICOS.* Citado por GONZALEZ NAVARRO, F. Comentarios a la ley.... Ob. cit., pág. 818.

(43) Un puntual e introductorio glosario de términos utilizados en la informática jurídica para abogados, incluido los elementos, dispositivos o soportes integrantes del "Hardware" y el "software", En: Revista Actualidad Aranzadi. Ed. Aranzadi. S.A. Pamplona. Núm. 2 de Enero de 1992, págs.1-4.

de lnformación propiamente dicho; y, 2. *Las unidades periféricas*, propiamente dichas, porque rodean, auxilian y complementan el procedimiento informático iniciado en la CPU (Central Procesing United) del hardware. Podemos clasificarlos, así: a) unidades periféricas de entrada de información (E/ o Input --I/--): teclado, el puntero electromanovisual o "mouse", lectores ópticos (lápices), tableros electrónicos, unidades de rayos infrarojos (eliminan cables), cámaras de vídeo (muy sofisticadas como la de vídeo digital Canon DM-MVI, videocámara que permite captar imágenes en movimiento y pasarlas luego al ordenador, en donde podrán editarse: seleccionar y retocar imágenes individuales, etc.) y todos aquellos que se elaboren en el futuro con este fin, b) unidades periféricas de salida de información (/S u Output: /O): Monitores o pantallas de ordenador, las impresoras, plotters, scanners, cámara de vídeo, etc.); y ,c) Unidades periféricas de

Entrada y Salida de información (E/S o I/O), tales como, el teclado o consola, el monitor, el scanner, los tableros y dispositivos ópticos, etc.[44].

Igualmente, son medios lógicos, logiciales o de *software,* los denominados programas de ordenador, utilizados en el procedimiento o tratamiento de la toda clase de información o datos. El software (parte blanda) es el término acuñado por el profesor *Scala* por oposición al término hardware o parte dura del ordenador. Sin embargo, este término como otros devenidos de la informática tiene traducciones poco afortunadas o vacía de entendimiento cuando se trasladan al castellano, por ello, es conveniente mantener el término inglés de software o el asimilatorio en castellado de programa de computador y no el de la traducción literal[45].

El Software o programa de ordenador *es toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una tarea u obtener un resultado determinado, cualquiera que fuera su forma de expresión y fijación* (art. 96 Ley de la Propiedad intelectual

---

(44) Un estudio más amplio en mi trabajo, *Constitución 1991 y la informática jurídica*... Ob. cit., pág. 128 a 234. Igualmente, con carácter didáctico, se han clasificado las unidades periféricas teniendo en cuenta la función que cumplen de la siguiente manera: a) *Primer Grupo*. Periféricos que establecen diálogos con el ordenador y a través de los cuales el usuario controla el sistema y guía las operaciones y da las órdenes a realizar, b) *Segundo Grupo*. Periféricos que actúan a manera de memoria auxiliar permitiendo guardar, con una estructura y organización determinada y adaptada a nuestro tipo de trabajo, la información para poder ser recuperada o leída con él y poder manejarla nuevamente, y c) *Tercer Grupo.* Periféricos que reciben información del ordenador en soporte de papel para generar un documento que puede ser considerado como definitivo y resultado de un proceso. En: Revista Actualidad Aranzadi. Ed. Aranzadi. S.A. Pamplona. Núm. 2 de Enero de 1992, pág.1

(45) Mi trabajo, LA INFORMATICA JURIDICA... Ob cit., pág. 195

Española. LPI).

En la definición se hallan inmersas algunas de las características más relevantes de los programas de ordenador. Estas son: a) Constituyen estructuras lógicas compuestas de cadenas de instrucciones previamente determinadas para conseguir un fin, b) Hacen posible el funcionamiento de un ordenador, pues esa serie encadenada de instrucciones indican al equipo computacional qué, cómo y cuándo se ha de efectuar una actividad o tarea propias del fenómeno electromagnético y mecánico, c) Pueden almacenar y recuperar información de cualquier tipo; y , d) Las tareas que realizan los programas de ordenador, son tan variadas como la imaginación y requerimientos

puntuales del ser humano. En las tareas que realizan los programas de ordenador podemos detectar además las funciones generales y específicas, inherentes a todo medio informático.

Una clasificación de programas de computador, que propusimos en otro momento [46], es la siguiente:

1. *Lenguajes de programación*. Se cuentan por niveles y generaciones. Sirven para facilitar el desarrollo de nuevos programas.v.gr. ALGOL (matemáticas), COBOL (comercial), FORTRAN (técnico-científico), PASCAL (aplicaciones generales), LOGO (aplicaciones infantiles);

2. *Programas de procesamiento, organización, cualificación y cuantificación de datos.* Proveen soluciones al procesamiento de textos, su organización, vinculación o fusión con otros, etc. v.gr. WORDSTAR, WORDPERFECT, WORKS DE MICROSOFT, PROFESSIONAL WRITE, WORD PROCESSING, etc., así mismo proporcionan soluciones al manejo de datos alfanuméricos, gráficos y contables, con posibilidades de fusión, intercambio o transferencia de datos. v.gr. LOTUS 123, QUATTRO, EXEL, etc.

3. *Programas operacionales.* Son los que permiten el funcionamiento, organización, control e intercomunicación del ordenador. Si se nos permite el símil, el programa de ordenador es el alma sin la cual el cuerpo (hardware) permanecerá muerto, al menos hasta estos momentos. El software sin el hardware, o viceversa, no son nada.

---

(46) Ibídem. Ob. ut supra cit. 199 y ss

Esto era tan evidente en los inicios de los PC´s (Personal Computer), cuando no existían los "hard Disk", que para arrancar un ordenador, previamente había que insertar el programa operacional (MS-DOS, perteneciente a la gran Familia de Microsoft: Disk Operation System), para que cargado el programa en la memoria del ordenador, se pueda comenzar a trabajar con otros programas de ordenador. Era la época del ordenador con programas en discos flexibles o de acetato. Hoy en día, ante la presencia de ordenadores con "Hard Disk" de gran volumen, diversidad, capacidad de almacenamiento, manejo y transferencia de datos e incorporados en la estructura mecánica computador, no parece tan evidente la falta que el programa operacional le hace al ordenador, pero sin embargo, lo sigue siendo a pesar de que no lo veamos, y muy a pesar también, de que actualmente los programas operacionales no tienen ni la estructura ni la presentación ni las funciones iniciales de éstos, que eran exclusivamente la de poner en funcionamiento "la máquina informática". En efecto, hoy los programas operacionales, son a la vez programas de ambientación que mejora la presentación, organización, accesibilidad y puesta en marcha de otros programas, a través de ventanas interactivas e intercomunicables (sistema

"*WINDOWS*"), mucho colorido, funcionalidad, y facilidad de acceso por medios iconos o gráficos que identifican la tarea o labor a realizar, según los requerimientos del usuario que puede elegir entre una o varias actividades a la vez (la "multitarea" en la misma pantalla-escritorio).

En 1998, Microsoft, lanza un producto denominado "Windows 98", que cumple las funciones primarias y avanzadas de un programa operacional y se le adiciona la posibilidad de ser un programa que permite la transferencia e intercomunicación de datos entre ordenadores, navegar por el espacio electrónico, sin fronteras, todo en un sólo paquete. Esto ha generado una demanda de los competidores (NETSCAPE, principalmente, básicamente por el monopolio que genera Microsoft al incorporar esta última función --transferencia de datos-- a la primigenia --servir de sistema operacional del ordenador-- [47]).

4. *Programas de Almacenamiento, Estructuración lógica y Recuperación de Información.* Son aquellos con los cuales por sistemas de programación inmersos en estos pueden crear, manejar, controlar y administrar bancos, bases o ficheros de datos, públicos o privados, institucionales, etc.v.gr. La familia de los programas de "*DBASE*".

---

(47) Vid. DIARIO EL MUNDO. Domingo, Mayo 24 de 1998. En la cita de pié de página 194 de la parte IV, comentamos lo pertinente.

5. *Programas de intercomunicación entre ordenadores.* Con ellos se puede conectar entre ordenadores situados en diferentes lugares del planeta, contando previamente para ello, con un equipo y aparato computacional idóneo, es decir, un ordenador, una línea telefónica, un MODEM (Modular/DEModulador de señales de comunicación), un operador de comunicación (v.gr. Telefónica en España, TELECOM en Colombia), un proveedor de acceso (v.gr. SIEMENS) y un proveedor de contenidos (v.gr. Biblioteca de cualquier universidad, entidad estatal o privada, etc).

6. *Programas pedagógicos y recreacionales.* Sirven como su nombre lo indica al mejoramiento del proceso enseñanza-aprendizaje a todo nivel educativo y al vastísimo campo de la lúdica, respectivamente.

Así mismo, se entienden como *medios*, todos aquellos aparatos o sistemas electrónicos que no haciendo parte estrictamente del hardware o el software, sirven a los fines y objetivos

informáticos, al complementar o potenciarlos. Tal es caso del conjunto de aparatos y sistemas de telecomunicaciones unidos a los eléctricos y/o electrónicos que sirven para captar, editar, emitir, y sobre todo, transferir imágenes, sonido o texto; o todo a la vez, pues al fin y al cabo todo, todo aquello que pueda representarse en forma binaria es *información*, bien representada analógica o digitalmente, como por ejemplo, las fotografías; o cualquier fuente de información que es representada en forma digital y proveniente de la voz humana, los sonidos cualquiera sea la fuente de producción, las imágenes fijas o en movimiento, etc.

La capacidad de estos medios físicos o lógicos para captar, procesar, editar y entregar información o datos por cauces electrónicos, informáticos o telemáticos, es lo que determina que estos medios se les denomine globalmente, a los efectos de éste trabajo investigativo, *medios informáticos* y según las funciones que desempeñen como *electrónicos o telemáticos*, si además del acceso, almacenamiento, procesamiento pueden con el auxilio de otros medios idóneos (hardware y software), transferir o teletransmitir cualquier flujo de información o datos, a velocidades y con formatos electrónicos de un lugar a otro, sin límites fronterizos o territoriales y contando para ello con una línea telefónica, un MODEM (Modulador/DEModulador de señales de comunicación) y una estructura de red de redes de información y comunicación como el internet, un operador de telecomunicaciones (v.gr. telefónica), un proveedor de acceso (v.gr. SIEMENS) y un proveedor de contenidos (v.gr. una biblioteca universitaria.)

La LORTAD, en su exposición de motivos, y en el sentido antes plantado, hace alusión a los medios informáticos cuando explica que "Partiendo de que su finalidad (referida a L.O 5/1992) es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos *por medios informáticos*...". Sin embargo, en el texto normativo, la ley guarda silencio en cuanto a qué se debe entenderse por medios informáticos, muy a pesar de que el ámbito objetivo de la LORTAD, se les vuelve a mencionar como mecanismos, instrumentos o elementos por los cuales se hace efectivo "el tratamiento automatizado" de los datos personales (art. 1), cuando es lícito o cuando se prohíbe sí estos son fraudulentos, desleales o ilícitos (art.4.7.).

En la parte IV, de este trabajo dedicaremos un apartado especial a los medios informáticos, electrónicos o telemáticos.

3. LOS "FICHEROS AUTOMATIZADOS" O BANCOS DE INFORMACION PERSONAL O BANCO DE DATOS.

En la presente sección abordamos el tema que en el ambiente del derecho comunitario europeo y español, se denominan "ficheros automatizados" (del francés: *fichiers automatiques*) para designar y conceptualizar lo que en el derecho anglosajón, en el ámbito de los Estados de la *Common Wealth* y el derecho americano se llama "Banco de información personal" (*personal information Bank)* o "Banco de datos personales" (*database*).

3. 1. El FICHERO COMO SOFTWARE Y HARDWARE EN LA LEGISLACION COMUNITARIA Y ESPAÑOLA.

Estudiaremos el *fichero* considerado como dispositivo inmaterial, lógico o de *software* y como elemento, soporte material o de *hardware,* continente de información o datos de carácter personal.

Los "*ficheros automatizados*", o mejor "*ficheros*", es otro de los términos que aparece continua y corrientemente en las normas jurídicas comunitarias y españolas, que regulan el tratamiento de la información o de datos por medios informáticos, electrónicos o telemáticos. Por ello conviene analizarlos a la luz del derecho y destacar algunas características, funciones y efectos que tiene en el procedimiento informático.

En la legislación española, principalmente en la LORTAD, se utiliza el término "fichero automatizado", para referirse a *todo conjunto organizado de datos de carácter personal que sean objeto de tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.* Estos datos pueden ser objeto de *operaciones y procedimientos técnicos, de carácter auto- matizado, que permitan la recogida, grabación, conservación, elaboración, modifi- cación, bloqueo y cancelación, así como las cesiones de datos que resulten de comu- nicaciones, consultas, interconexiones y transferencias* (LORTAD, art. 3, b), y c),).

En este sentido, el fichero es considerado como un programa de computador o software, puesto que desempeña las funciones típicas y contiene también características de aquéllos. En efecto, el fichero como el software permite ingresar o acceder, almacenar, procesar y transmitir información o datos, siempre que se disponga de unos elementos, dispositivos o aparatos computacionales o medios informáticos, electrónicos o telemáticos. Por esta última razón sobra

post incluir el término "*automatizado*" al fichero, pues el sólo *nomen* técnico-jurídico, indica que las funciones realizadas con la información son de carácter electromagnético o desactualizadamente de carácter "automático". Más aún, las mismas normas comunitarias europeas diferencian entre "fichero" y " *carpeta* ", para indicar con esta última la forma mecánica o simplemente manual de almacenar o recuperar información de carácter personal (Considerando 27, Directiva 95/46/CE), con lo cual el término automático, sigue sobrando, como ampliaremos más adelante.

El software es el nombre genérico de toda estructura lógica creada y utilizada para desempeñar este tipo de funciones exclusivas de todo programa de ordenador; en cambio, el fichero es el nombre específico de una clase de software con iguales funciones y con fines y propósitos específicos, según los creadores y los usuarios correspondientes, bien sean públicos o privados. En nuestro caso, el término *fichero* a que hacen mención las normas jurídicas, por regla general, se entienden como los ficheros de información personal o de datos de carácter personal, pues han sido creados para almacenar y recuperar *cualquier tipo de información considerada personal o familiar*, según el ordenamiento jurídico vigente de los Estados.

Igualmente software y fichero tendrán similares características dentro del ámbito de género y especie de los términos. Algunas de las más relevantes características, son: a) La lecto-escritura de los programas de computador sólo puede ser posible con medios computacionales; b) Las funciones que permiten grabar, conservar, bloquear o cancelar registros informáticos o datos, pueden realizarse por uno o varios usuarios, independientemente de si están o no autorizados, siempre que estén ante equipos electromagnéticos idóneos o cuenten con aparatos que intercomuniquen a dos o más ordenadores; c) Los programas de computador para cumplir sus fines y propósitos, generales o específicos deben necesariamente disponer de un equipo u ordenador, es decir, software y hardware, son un duo inseparable.

Por estas razones, tanto la LORTAD, las normas desarrollo como en el ámbito del derecho penal español, el término "fichero", utilizado por el art. 197.2. del C.P.Esp., es considerado, a la luz de la informática, como un programa de ordenador, puesto que como todo programa de ordenador facilita o complementa un conjunto de operaciones, instrucciones, tratamientos y *comunicación de datos o informaciones del hombre con la máquina en forma automatizada, o entre ordenadores* en forma electrónica o telemática. En efecto, todas las actividades relacionadas en el art. 3, con los ficheros son funciones y atribuciones propias de los

programas de ordenador a las cuales tienen acceso, tanto el hombre (STC 328/1998, Enero 1. FJ.4, "*programa informático"*) como el ordenador mismo.

En la Legislación Comunitaria Europea, particularmente en el Convenio Europeo de Estrasburgo de 1981, el fichero es considerado también como un programa de computador, puesto que se refiere al "fichero automatizado" como a "*cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado*" (art.2-b,), entendiendo por tratamiento automatizado como "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,). Estos ficheros o programas de computador serán controladas por una autoridad erigida al efecto y representada por una "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 automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán" (art. 3-d,). Una de las características de los programas de computador, como de los ficheros es la que determina, entre otras, el Convenio sobre la Seguridad de los datos. En efecto, se dice: "se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados (art.7).

Por su parte, la Directiva 95/46/CE, al extender la aplicación de la protección de las personas tanto al "*tratamiento automático*" de datos como a su tratamiento manual, explica la diferencia entre lo que considera como "fichero" y "carpeta", como las diferentes formas de almacenar, organizar y recuperar información o datos: por tratamiento automático, el fichero; por tratamiento manual, la carpeta. Aunque, a renglón seguido en el considerando 27, aclara que 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 Directiva sólo abarca *los ficheros*, y no se aplica a las carpetas que no están estructuradas.

Insiste la Directiva que 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. Finalmente, sostiene 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

Por su parte, la Directiva en su parte normativa sostiene que "fichero de datos personales" o simplemente "fichero", es *todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.* (Art. 2, c), Directiva).
Con lo cual se destaca tanto las funciones como características de todo programa de ordenador y le adiciona unos conceptos jurídicos propios del ámbito del derecho administrativo para determinar el ámbito de competencia territorial y funcional de los ficheros, que a la vista de las nuevas tecnologías de la información y de la comuni- cación (TIC), quedan totalmente desfasados, pues ya hemos dicho que están tienen como característica principal, la de comunicarse entre ordenadores por medios electro- magnéticos idóneos, sin fronteras y sin límites territoriales. Quizá los términos de com- petencia funcional y territorial, sirvan para la determinación de las autoridades que ejer- cen el control y administración de los ficheros en los diferentes Estados, y nada más.

El fichero como conjunto estructurado de datos, tiene una tratamiento informático previo, que se concreta en *cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados, y aplicadas a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por trasmisión, 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, Directiva). Dicho tratamiento puede ser realizado por *una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento* (Art. 2-e Ibídem). Todo lo cual comprueba que el fichero tiene la vocación de programa de ordenador o software, por ser obra humana con conocimientos especiales, por autorización consentida o por ministerio de la ley, y además, porque cumple funciones, características y fines que exclusivamente pueden realizarse con los programas de ordenador, siempre que se disponga de un equipo computacional o electromagnético idóneo que tenga incorporada además la tecnología TIC.

El fichero tanto en la legislación española como comunitaria europea, también puede considerarse como un dispositivo, aparato o elemento computacional de carácter material, físico o

de “hardware”. En efecto, cuando en la legislación o jurisprudencia se hace mención al disco o disquete (del francés: *disque* y/o del inglés: *diskette*), como elemento material informático, fabricado de un delgado plástico (o acetato), recubierto de una fina película de material magnetizable, permeable, flexible que permite la escritura y lectura de forma también electromagnética [48], como también borrar o cancelar, modificar, nombrar o renombrar archivos o *files*, suprimir o transladarlos dentro y fuera del disco, o igualmente almacenar y recuperarlos según la capacidad, tamaño y especificaciones del disco.

En cuanto a la capacidad es variable, pues los primeros discos flexibles (*floppi*

---

(48) AA.VV. *INTRODUCCION A LA INFORMATICA (II)*. Ob. ut supra cit., pág. 2

disk), almacenaban información o datos desde 320.000 bytes [49] hasta 1.2 *Megabytes* (MB), si tiene un formato de disco de 5 1/4" (pulgadas), o de 730.000 bytes hasta 1.4. Megabytes, si el tamaño es de 3 “ (pulgadas). Es decir, que un disco de 5 1/4 cabría un libro de 450 páginas, a doble espacio, con sus correspondientes citas de pié de página. En un disco de 3 pulgadas, podríamos archivar, registrar o almacenar alrededor de tres libros de 450 páginas, cada uno. Hoy en día, existen programas de ordenador que doblan la capacidad de los discos flexibles y los propios “hard disk”, con lo cual se duplica su capacidad de archivo. Esta duplicación es virtual,. no real v.gr. comando “*double space*”, en MS-DOS, ver. 3.2.

Sin embargo, la tecnología informática para mejorar la capacidad, la clase de información almacenada (no sólo texto que era lo que básicamente podían almacenar los *floppi disk*, sino además imágenes, sonido, video o gráficos) e incluso la calidad y posibilidad de conservar mejor y más segura la información, se crearon los llamados discos compactos, “*compac disk*” o “CD´s”. Estos discos al principio tenían una capacidad de un “hard disk” de los años 86, es decir, con capacidad de 100 Megabytes (MB), luego y muy rápidamente por las necesidades de los usuarios, los productos ofrecidos y la competencia entre las empresas productoras de los mismos (v.gr. SONY, PHILIPS, HITACHI, TDK, IBM, etc), comenzaron a aumentar su capacidad 200, 500, 720 MB, y así sucesivamente con el paso del tiempo, hasta los de 2.000 MB, denominados LP, puesto que pueden ser leídos con un láser óptico [50]. Estos CD´s inicialmente fueron sólo de lectura (Only ready) ,y por ello se llamaron CD-ROM

---

(49) *Bit y Bytes*. Los ordenadores o computadores trabajan en sistema binario (0-1) y no decimal. Esto significa que lo hacen a través de "cambios e impulsos electrónicos" que compilan todas las operaciones, funciones y procedimientos lógicos en su memoria. Esto se conoce como "lenguaje de máquina". El computador cuando destella ceros, significa que hay ausencia de impulso, y si son unos, hay presencia de éstos. Esta función es similar a la de un commutador eléctrico que a la presión digital deja o no pasar electricidad, pero cada tiempo es diferente. "Un computador entiende como la unidad mínima de información a un *bit*, es decir, un cero y un uno. Sin embargo, un bit es una unidad demasiado pequeña como para almacenar suficiente información. De ahí aparece el *byte* que agrupa a *8 bits y* que ya puede ser el conjunto de, por ejemplo, 8 letras que conforman una palabra, un símbolo o una cifra". AA.VV. *CONOZCAMOS AL COMPUTADOS*. Ed. Kernel, Bogotá, 198(?), pág. 1. Citado en mi libro: LA INFORMATICA... Ob.cit., pág. 137.

(50) AA.VV. *INTRODUCCION A LA INFORMATICA (II)*. En: Revista Actualidad Aranzadi, Ed. Aranzadi S.A. Núm. 2, Enero, Pamplona, 1992, pág. 2..

(Random Only Memory) [51], luego con el paso del tiempo en la década de 1990, se incursionaron en el mercado los discos compactos de lectura y escritura, conocidos como CD-RAM, y últimamente, los DVD (Discos Digitales de video o Discos Digitales versátiles) [52], que pueden almacenar seis o siete veces la capacidad de un CD de principios de la década de los noventa, con la ventaja que además de almacenar texto, imágenes, sonido, tiene capacidad para almacenar una película de video, con todos sus efectos y características de cualquier película de video y con las potenciadas propias de un dispositivo, aparato o elemento informático v.gr. Editar, modificar, borrar, etc., secuencias o datos digitalizados de texto, imagen, sonido o audio.

Finalmente, en el concepto de disco como objeto material continente de información digitalizada (texto, imágenes o sonido), por lo dicho cabe el llamado "hard Disk" o disco fijo o no removible, con capacidad, estructura y modelos tan diversos como la imaginación humana.

El Tribunal Supremo Español, en varias sentencias se ha referido al fichero como hardware, cuando ha querido definir el "*documento informático*" por asimilación del documento general y por vía de ejemplo, cita a " *un disquete*" como continente material de información o datos y no como contenido o más aún que exprese la clase de contenido de aquel. Así lo podemos constatar en la Sentencia de Noviembre 23 de 1996 y las sentencias referidas en aquella [53].

---

(51) "Técnicamente, el CD-ROM se construye igual que el CD-Audio: aquí también encontramos la técnica del *pit y land* (es decir, la técnica de lectura que tienen los videodiscos que como sistemas ópticos se hace utilizando un haz de luz que lee un dato codificado a partir de aberturas (pits) y superficies planas (lands) organizadas en espiral y no en círculos concéntricos como los disquetes)... Del CD-Audio se ha pasado al CD-ROM mediante una nueva pauta acordada con los japoneses acerca del modo de escribir otros datos fuera de la música. En verdad, si en música se pierde alguna información, no se producen interrupciones: el sistema analiza el dato precedente y el dato que sigue al que se perdió, y luego intercala el valor faltante; el oído humano no percibe ninguna discontinuidad. Esta técnica no es aplicable a otro tipo de datos. Entre una *'a'* y una *'c'* no se puede saber qué hay;

por tanto, era necesario proveer mayores garantías a la recuperación de errores. Hoy se produce un error cada 10^{15} bit; es decir, que falla un carácter cada mil billones de caracteres --prácticamente no hay error--. Así, la seguridad que ofrece el disco compacto es excepcional." LOSANO, Mario. *DE LA PLUMA DE GANZO AL RAYO LASER:NUEVAS TECNOLOGIAS PARA LOS BANCOS DE DATOS Y LAS EDITORIALES*. En: INFORMATICA Y DERECHO. Aportes de doctrina Internacional. ALTMARK, Daniel y BIELSA, Rafael. Ed. Depalma. Buenos Aires, Argentina, 1988, pág.101 y ss.

(52) El DVD. Vid. Diario EL MUNDO, Domingo 5 de abril de 1998, págs. 12 y 13.

(53) Vid. AA.VV. *COMPEDIO DE DISCOS ARANZADI*. Ed. Aranzadi, Pamplona, 1998.

3.1. LOS BANCOS DE DATOS COMO ESTRUCTURAS LÓGICAS DE ALMACENAMIENTO, PROCESAMIENTO Y RECUPERACION DE LA INFORMACIÓN O DE DATOS..

Los bancos de información personal (*Personal Informatio Bank*) o simplemente bancos de datos ("*database*"), son términos que el derecho Anglosajón, el del ámbito de los Estados de la *Common Wealth y* el derecho americano ha incorporado en sus textos normativos con idénticas funciones, característica y propósitos a la de los *ficheros como programas de ordenador o software.* Los Bancos de datos son programas de ordenador, que a los efectos de este trabajo investigativo los hemos clasificado y conceptuado como programas de almacenamiento, estructuración lógica, administración, control y recuperación de información de carácter personal.

La *Privacy Act* 1988 [54] Australiana, define a la "Información personal" como toda información u opinión, verdadera o no, de una persona identificada o identificable, incluida la que hace parte de un banco de datos ("*database"*), registrada o grabada en forma material o no (art. 6). v.gr. Los registros o archivos del número de identificación tributaria de una persona. Similar definición se relaciona en la *Privacy and Data protection Bill 1994*, en el art. 3, destacando que también se considera información personal los datos, documentos o asimilables, registros o archivos ("records [55]") contenido en un Banco de Datos. En esta ley de la *Common Wealth,* con mayor razón se destaca esta estructura lógica de la información, cual es, el banco de datos, pues es una norma jurídica especializada en la protección de la intimidad y de los datos procesados por medios informáticos, electrónicos o telemáticos. En consecuencia, en el derecho australiano se instituye una protección genérica y otra específica de los datos o información personal contenida en los Bancos de Datos.

La Ley de protección a la intimidad Canadiense --LPDPC-- (*Privacy Act*), define la información personal o datos personales, como toda información concerniente

---

(54) Texto completo En: *WWW. AUSTLLI. EDU.AU.* Biblioteca Virtual de Derecho de la Universidad "Austlli" de Australia. Vía internet. Inglés. 1998

(55) Ley del derecho de acceso a la información Canadiense . (Access to information Act 1983), art. 3., considera como registro ("*record*") a la información o datos contenidos en un documento, cualquier correspondencia, memorándum, libro,

plano, dibujo, diagrama, trabajo pictórico o gráfico, fotografía, filmación, microfilmación, grabación, video, registros leíbles mediante aparatos ("machine readable record"), y cualquier otro material documental, sin tener en cuenta la forma física o sus características, así como cualquier copia que de estos se realice. En: *WWW. UMONTREAL. EDU. CA.* Biblioteca Virtual de Derecho de la Universidad de Montreal Canadá, vía internet. Inglés-francés. 1998.

a una persona cualesquiera sean los mecanismo de obtención o en que se graben. A renglón seguido, incorpora un extenso listado *numerus clausus* (trece literales [56]), fuente de información considerada personal, sin distinguir legislativamente si unos datos son más o menos sensibles, o si deben prodigárseles más o menos grado de protección, pues se sigue la regla general de que una información personal, sólo puede ser descubierta o divulgada, si existe consentimiento de la persona concernida o así lo dispone la ley, siempre que la información este bajo el control o responsabilidad de una autoridad estatal y se trate una cualquiera de las trece situaciones previstas en el art. 3 LPDPC. (Mackenzie v. Canadá --Ministerio de Salud Nacional y Bienestar Social. 1994, 88 F, T.R.52; 59 C.P.R. Primera Instancia. Corte Federal).

Por su parte, la mencionada *Privacy Act* del Canadá, en el art. 3., define el banco de datos ("personal information bank" o "fichier...") como todo conjunto, colección o agrupamiento de información. Esta información puede ser consultada o _____

(56) Se considera información personal, la siguiente: "**(a)** information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, **(b)** information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, **(c)** any identifying number, symbol or other particular assigned to the individual, **(d)** the address, fingerprints or blood type of the individual, **(e)** The personal opinions or views of the individual except where they are about another individual or abouta proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, **(f)** correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, **(g)** the views or opinions of another individual about the individual, **(h)** the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and **(i)** the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include **(j)** information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including: 1) the fact that the individual is or was an officer or employee of the government institution, 2) the title, business address and telephone number of the individual, 3) the classification, salary range and responsibilities of the position held by the individual, 4) the name of the individual on a document prepared by the individual in the course of employment, and 5) the personal opinions or views of the individual given in the course of employment, **(k)** information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services, **(l)** information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and **(m)** information about an individual who has been dead for more than twenty years". Texto de la ley completo en: *WWW.UMONTREAL. CANADA. CA.* Biblioteca Virtual de Derecho de la Universidad de Montreal Canadá, vía internet. Inglés-francés. 1998.

recuperada por medios informáticos, siempre que se halle bajo la responsabilidad y control de una autoridad estatal, esté disponible para los usuarios, se solicite con fines administrativos y se referencia el nombre, el número o cualquier otro símbolo que iden-
tifique plenamente a la persona concernida o haga posibilite su identificabilidad. Se exceptúa de tales solicitudes, la información contenida en los bancos de datos del Archivo Nacional del Canadá (*National Archivist of Canada*), registradas, relacionadas, archivadas o transferidas a la institución gubernamental para fines históricos. (Art. 10-1, 10-2)

Ahora bien: Los Bancos de datos desde la óptica de la informática jurídica documental, se han clasificado [57], así: 1. Por el cantidad de la información almacenada, en: a) Bases de datos textuales, b) Bases de datos referenciales, c) Bases de datos factuales; 2. Por el lenguaje adoptado en el almacenamiento de la información, en : a) Bases de datos sustentadas sobre el lenguaje natural, b) Bases de datos sustentadas sobre lenguajes documentales, y c) Bases de datos mixtas; 3. Por el contenido de la información almacenada, en: a) Bases de datos legislativas, b) Bases de datos jurisprudenciales, c) Bases de datos doctrinales, d) Bases de datos parlamentarias; 4. Por la cobertura temática, en: a) Bases de datos sectoriales o modulares, b) Bases de datos multisectoriales, y c) Bases de datos multidisciplinarias.

A nuestros propósitos, nos interesa hacer mención de los bancos de datos clasificados según el lenguaje adoptado en el almacenamiento de la información, particularmente los bancos de datos en lenguaje no documental y documentario, ya que los bancos de datos mixtos al ser el producto necesario de los dos, utilizan sus ventajas, funciones y características fusionadas.

Los Bancos de datos en lenguaje no documental o natural: son aquellas en las que el tratamiento de la información se realiza mediante sistemas que permiten efectuar diferentes aplicaciones informáticas, utilizando las palabras del título, texto o resumen de los documentos almacenados, sin precisar de ningún proceso documental añadido a dicha información [58].

---

(57) Cfr. PAEZ MAÑA, Jorge. *COMENTARIOS SOBRE ALGUNAS PARTICULARIDADES DE LAS BASES DE DATOS JURIDICAS*. En: Revista Actualidad Aranzadi. Ed. Aranzadi S.A., Núm. 16, Julio, Pamplona, 1995, pág. 5 y ss.

(58) Ibídem, pág. 5, ss.

Los Bancos de datos en lenguaje documental: son aquellas en las que predominan las aplicaciones informáticas tendentes a recuperar y tratar la información en ellas almacenada, utilizando los términos documentales (palabras claves, descriptores, thesaurus, etc.) elaborados a

partir del análisis de su contenido, siendo accesorias, a efectos de recuperación, las aplicaciones utilizadas sobre las partes que conservan su lenguaje original (título, notas, etc) [59].

Las finalidades que persiguen las bases de datos continentes de información personal y que estén bajo el control, manejo y administración de una persona natural o jurídica, institución pública o privada responsables, por lo visto, serán:

a) Que la variada información considerada de carácter personal, sea compilada, clasificada, organizada en forma legítima, por personas naturales o jurídicas o instituciones públicas y privadas para fines actuales o *a posteriori* lícitos de recuperación, transferencia (cesión o divulgación) por medios informáticos, electrónicos o telemáticos, por quien , a su vez , esté autorizado por mandato judicial, disposición legal o porque le concierne a él;

b) Para que permanente, continua y corrientemente, se actualice, modifique, aclare, cancele o borre la información, siempre que preste su consentimiento el titular de la información o el concernido, o lo imponga un mandato judicial o por disposición de la ley;

c) Para que el acceso a la información estructurada lógicamente en un banco de datos, sea fácil, rápido, eficaz, oportuno, libre obstáculos técnicos y engorrosos (característicos de la información compilada en forma manual o mecánica), por parte de los usuarios, siempre que se disponga de medios informáticos idóneos o telemáticos idóneos, autorización legal o por mandato judicial, y más aún, sin estar físicamente presente en el lugar o espacio locativo donde se encuentre el banco de datos, si el acceso o recuperación de datos es requerido por un usuario que se halla en un espacio territorial diferente o que no coincide en nada con la división geopolítica del país donde se halla la

---

(59) Ibídem, pág. 5, ss.

información solicitada. v.gr. La información solicitada, vía internet con medios informáticos y telemáticos idóneas, por un usuario que se halla en la ciudad de San Juan de Pasto (Colombia), de un dato académico *in situ* en la base de datos de estudiantes del tercer ciclo de enseñanza universitaria de la Universidad de Lleida (España). La información será entregada a velocidades y formatos electrónicos, si está autorizado para el acceso y la consulta;

d) Que los sistemas de acceso como de recuperación de información por medios informáticos sea idóneo y permitan una vez dentro del contenido de la base de datos la búsqueda fácil y ordenada por palabras claves, descriptores, términos relacionados, prefijos o sufijos relacionales, etc. En fin, que permita al usuario acceder y recuperar los datos de forma clara, precisa y actualizada;

e) Que se incremente la seguridad jurídica y unidad de materia compilada legítimamente en un banco de datos y toda clase de medidas, instrumentos y mecanismos de protección y garantía de los derechos, libertades públicas e intereses legítimos, básicamente para el concernido, los usuarios y los responsables del control, manejo y administración de los bancos (personas naturales o jurídicas, institucionales o corporativas de carácter particular o público);

f) Que se estructure lógicamente toda información considerada personal, salvo la que por disposición del mismo ordenamiento jurídico vigente, se prohíba, limite o restrinja su compilación o se sometan al procedimiento de disociación para que el dato no se asocie a una persona determinada v.gr. Los denominados "*datos sensibles*" o correspondientes al "*núcleo duro de la privacy* [60]", tales como el origen racial o étnico, ideología, religión, creencias, salud o vida sexual, inicialmente está prohibido su tratamiento por medios informáticos, electrónicos o telemáticos (art. 6 del Convenio de Estrasburgo de 1981; art. 8 de la Directiva 95/46/CE), podrían compilarse en bancos de

---

(60) Según FROSINI, V. *BANCHE DEI DATI E TUTELA DELLA PERSONA, pág.* 15., citado por MORALES PRATS, Fermín, en *LA TUTELA PENAL DE LA INTIMIDAD: PRIVACY E INFORMATICA*..Barcelona (Esp.), 1984, pág. 61. Ibídem., *DELITOS CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y LA INVIOLABILIDAD DE DOMICILIO.* En: Comentarios a la Parte Especial del Derecho Penal. Ed. Aranzadi., Pamplona, (Esp), 1996, pág. 32l.

datos, siempre y cuando, se sometan al procedimiento de disociación de la información (art. 3-f, LORTAD), de lo contrario, será, cuando menos, ilegítima e ilegal sino existe consentimiento claro, expreso y escrito del titular o concernido, lo autorice el ordenamiento jurídico o un mandato judicial (*Privacy Act*., art.3, y *Access to information Act Canadiense*, art. 19). Más aún, será inconstitucional [61].

g) Que se distinga claramente el diferente grado, ámbito competencial y nivel de protección social y jurídica que debe dispensarse a los Bancos de datos contentivos de

información considerada legalmente personal (o "sensible" por la doctrina) y los Bancos de datos con información personal pero con acceso colectivo a la misma por primar en esta última clase de información el interés público sobre el privado. En efecto, sobre la información de tipo económico, estadístico o científico, cuya esencia es la de ser *impersonales,* prevalecerá el derecho a la información *"a través del reconocimiento del derecho al acceso colectivo a los bancos de datos, entendiendo que este derecho constituye hoy una de las manifestaciones más importantes del derecho a la información, en cuanto derecho activo o derecho-participación en los procesos decisorios de la ordenación política, económica o social de una comunidad"* [62] .

Esta última finalidad de los bancos de datos, también sirve para distinguir, al menos en el plano conceptual, tres tipos de datos susceptibles de tratamiento informático, aún cuando la regla general es que cualquier clase de datos de carácter personal puede ser sometido a tratamiento informático, electrónico o telemático, salvo las prohibiciones, restricciones o limitaciones puntual y expresamente previstas en el ordenamiento jurídico vigente en cada Estado, y en el plano europeo además, según las recomendaciones, normas comunitarias (v.gr. Convenio Europeo de 1981) y Directivas (v.gr. 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*).

Esta clasificación conceptual de datos, planteada por el profesor *Morales Prats* [63], es como sigue: a) Los relativos al denominado *núcleo duro de la intimidad,* b) Las informaciones que siendo de carácter personal (nombre, apellido, domicilio...), pueden entrar en el ciclo informático, siempre y cuando por esta cesión de información

---

(61) Este aspecto, lo tratamos con amplitud en la Parte I, de este trabajo.

(62) Vid. MORALES PRATS, Fermín, en *LA TUTELA PENAL DE LA INTIMIDAD: PRIVACY E INFORMATICA*..Barcelona (Esp.), 1984, pág. 61 y ss.

(63) Ibídem, pág. 61 y ss.

el individuo obtenga contrapartida en orden al derecho a controlar cómo almacena, procesa y circula esa información, lo que significa: el acceso restringido al banco de datos, el derecho de rectificación de datos inexactos, el derecho de cancelación de informaciones potencialmente perjudiciales (el derecho de *habeas data*). Permiten el mantenimiento de la exactitud y confidencialidad de los datos, proporcionados al centro informático por razones de interés público o cualesquiera otros de carácter lícito. El manejo de esta información por los responsables conlleva especiales deberes como el de sigilo y diligencia profesionales (*sigilium professionalis), y* c) El resto de información, susceptibles de ser tratadas por impulsos electrónicos, queda constituido por los datos anónimos, económicos o científico-estadísticos. Del conocimiento y acceso a estas informaciones no depende el derecho a la intimidad, sino intereses colectivos,

centrados en la existencia de presupuestos de hecho que faciliten la socialización de la información. El habeas data del ciudadano no se compone exclusivamente de derechos que emanan de la privacy, sino también de facultades entroncadas con el derecho de la información. Por ello, la institucionalización de vías procedimentales que faciliten el ejercicio de estas últimas, mediante el acceso generalizado a las fuentes de información que constituyen los bancos de datos, afecta a los procesos de democratización de los sistemas políticos. Por ello, *el control colectivo del tratamiento informático de estos datos es, pues, incontrovertible* [64].

4. EL DOCUMENTO ELECTRÓNICO Y/O TELEMÁTICO.

4.1. LA CULTURA ELECTRONICA: LA REDEFINICION DE LA INFORMACION.

El profesor *Ethain* [65], explica que el actual "*nuevo ambiente tecnológico*" en el cual estamos inmersos genera una especie de "*cultura electrónica*", que encuentra su fundamento en las predecesoras "cultura de la escritura" y la "cultura de la impresión o del libro", en tanto en cuanto éstas, le han proporcionado los elementos esenciales de la intercomunicación entre seres humanos: el idioma como canal, la escritura y la impresión como medios idóneos de la misma y los instrumentos mecánicos de comunicación como accesorios de expansión, difusión y divulgación de las ideas, pensamientos, sentimientos y conceptos.

---

(64) Ibídem, pág. 61 y ss.

(65) KATSH, M. Ethain. *RIGHTS, CAMERA, ACTION: CYBERSPATIAL SETTINGS AND THE FIRST AMENDMENTET*. Professor of legal Studies, University of Massachusetts at Amherts; B.A. 1967, NewYork University, J.D, 1970, Yale University. 1995. Texto Completo en WWW.UMONTREAL.EDU.CA.

Sin embargo, el nuevo ambiente tecnológico está compuesto básicamente por cuatro elementos que interactúan entre sí para producir los fines y propósitos que diferencien la cultura de la impresión de la cultura electrónica. Siguiendo al profesor Ethain, estos son:

a) *Los computadores interconectados a una red de redes de información*. Estos constituyen los mecanismos para la distribución electrónica y la publicación. Las redes de computadores que se nutren entre sí están interconectadas, con lo cual constituyen la "culminación de un proceso evolutivo que puede decirse tiene cinco etapas: a) el traslado de archivos, registros o información, b) Lugares lejanos conectados entre sí, c) sistemas computacionales de redes electrónicas de distribución de información, d) trabajo intelectual en colaboración y en tiempo real, y e) la concordancia entre la utilización de recursos humanos y técnico-electrónicos para obtener un servicio rápido y eficaz" [66].

En la primera etapa, una red puede transferir archivos de información entre computadoras, pero sin garantizar el tiempo de la entrega. Esta etapa es suficiente para apoyar el correo electrónico (*E-Mail*), los tablones de anuncios (*bulletin boards*), servicio de noticias (*news services*) y los periódicos autorizados.

En la segunda etapa, la red permite al usuario conectarse a través del ordenador con recursos remotos o lejanos, por ejemplo, con un banco de datos in situ en un lugar distante. La consulta y el empleo de los recursos es en tiempo real (*real-time*), como si se estuviera en el sitio y la hora del lugar consultado.

En la tercera etapa, la red esta disponible al usuario como soporte en los procesos computacionales e incluye también los recursos a los procesos computacionales entre *"NODOS"* (terminales de señales de comunicación para ordenadores) bastante distantes. v.gr. un proceso de comunicación interface por parte de un usuario conectado con un terminal a un supercomputador, conectado a su vez, con un computador que despliega medios visuales o gráficos.

En la cuarta etapa, la red le permite al usuario disfrutar directamente y en

---

(66) DENNING, Peter. *A NEW PARADIGM FOR SCIENCE*, 1987. Citado por Ethain Kasth, Ob. ut supra cit. sin dirección electrónica.

colaboración con otras personas en tiempo real de diferentes utilidades a través de diversos medios o terminales, tales como las conferencias que le permiten participar activamente en ellas, compartir un "*universo común*" en el que pueden hablar, interpelar, solicitar la revisión de todo o parte del contenido mediante la ejecución de programas de computador que examinan las entradas y salidas de información (exámenes de rendimiento).

En la quinta etapa, el conjunto de recursos (humanos y técnicos) y medios permiten un sistema coherente en el que todos contribuyen y reciben satisfacciones. Cada persona puede mirar a través de un terminal de computadoras un mundo de información. La red le proporciona muchos servicios que le permiten al usuario localizar, acceder, utilizar y contribuir con sus propios recursos en una multitud de disciplinas.

En la actualidad todavía estamos distantes de la fácil utilización y flexibilidad de estos recursos y medios que proporciona la comunicación electrónica. Algunas de las primeras etapas

descritas si se han asimilado por muchísimas personas en el mundo, pero falta mucho más por comprender. El mundo del *On line* se ha vuelto un lugar más habitable cada día, pero aún no es tan accesible, amigable y de fácil utilización como se pretende. La información electrónica basada en la red podrá ir creciendo tal como sucedió con los cajeros automáticos (“*automatic teller machine”)* que hoy constituyen un ejemplo cotidiano de un acceso amigable, de fácil utilización y de comunicación a velocidades y formatos electrónicos. Hoy, todavía existen barreras de “hardware” y “software” que no permiten, todavía masificar la comunicación para conseguir una información.

La red de redes de información conocido como *Internet*, ha experimentado un crecimiento geométrico, a pesar de los muchos obstáculos técnicos que aún subsisten. v.gr. En 1988, el número de redes conectado a internet en USA era de 217, en Octubre de 1994, era de 4.852.000.

El ordenador conectada a una red de computadores cambió la distribución de la información de un sistema dependiente de los medios de transporte a un proceso de información que se mueve a velocidades electrónicas, que superan los límites de velocidad de aviones, trenes, etc, e incluso sobrepasan fronteras territoriales que antes interferían en la comunicación de esa información. Esto provocó una “redefinición de la información. La velocidad, rapidez y desplazamiento de la información, sin límites geográficos, bien puede representarse con la frase de *Michael Benedikt*, cuando dice: “Puedes vagar por el mundo sin abandonar nunca tu casa” [67].

El cambio de las redes electrónicas de comunicación, se nota no sólo en la dimensión espacial y facilidad de emitir y recepcionar información, sino más aún, en la dimensión temporal, pues es aquí donde más cambios profundos se produce. Las redes electrónicas permiten acceder a mucha más información a la cual antes era inaccesible y generalmente sin pagar ningún valor y aún cuando se halle muy distante y todo esto es posible en el mismo instante que se solicita por la red. Igualmente, los usuarios de la información podrá mantener unas relaciones “distantes” de trabajo colectivo como si fuesen co-obreros (“*co-workers”)* que pueden actuar reciproca y eficazmente sin estar físicamente juntos. La información se comparte, amplia y potencia en estas nuevas relaciones interpersonales o luego institucionales.

Somos una sociedad cada vez más conectada con redes electrónicas pues cualquier computadora que se halle conectada beneficia la interacción de forma ilimitada a otras situadas en diferentes lugares. Un individuo no conectado a una red es una persona aislada, y cada vez menos capaz de dar valor a una información o de trabajar en equipo. Bien es cierto que las redes no

pueden satisfacer todas las necesidades que son satisfechas en una comunicación cara a cara ("*face-to-face*"), pero estas satisfacen la mayor parte de ellas sin estar físicamente presentes.

El correo electrónico, por ejemplo, para un gran número de personas es un medio de comunicación inconveniente frente al teléfono o mejor aún ir caminando por un pasillo hasta la oficina de un abogado o colega. Sin embargo, día a día va creciendo la necesidad de este medio electrónico de comunicación. Cuando ocurra el cambio, se dimensionará las relaciones de la cultura electrónica, que utiliza medios, recursos, distancias y velocidades igualmente electrónicas. Utilizar información o datos en este ambiente electrónico significará virtualmente que no hay diferencia entre utilizar la información en el lugar que se produce, proporciona y hacerlo en su propio computador.

b) *La comunicación interactiva generada por personas que están conectadas a una red de información*. Esta comunicación es bidireccional, pues los mensajes transmitidos y recepcionados en diferentes lugares a velocidades y formatos electrónicos

---

(67) Cfr. "wander the earth an never leave home". BENEDIKT, Michael. *INTRODUCCION TO CYBERSPACE: FIRST STEPS*, 1991. Citado por Ethain Kasth. Ibídem. Sin dirección electrónica.

con contenidos de texto, imagen, sonido y vinculaciones a otros documentos a la vez, situados en terceros lugares a los del emisor y receptor, diferencian grandemente la comunicación que se generaba en la lectura de un libro, revista, etc., en fin, en la cultura de la impresión;

c) *La palabra y la imagen*. El libro ilustrado es un ejemplo típico de la dualidad de la palabra e imagen, de la comunicación textual que ha ido creciendo ampliamente en la cultura de la impresión. Sin embargo, la imagen sólo era la representación de la palabra o la potenciación de la misma. La televisión, aumentó la comunicación visual y auditiva, frente a la comunicación textual, sin embargo, no proporcionó al usuario o destinatario de la comunicación trabajar con los datos recibidos a través de ese medio. Los nuevos medios de comunicación proporcionan a los usuarios nuevas y mejores herramientos gráficas interactivas. Estas herramientas permiten bajar costos y reducir obstáculos en la comunicación, a través imágenes, iconos, mapas, figuras, gráficos, ventanas, escritorios de pantalla, bocetos, cianotipos, dibujos animados; en fin, muchas otras formas visuales. Las personas, colectivos o instituciones con estas nuevas herramientas visuales les permite aumentar su persuasión, descripción, representación, caracterización propias de un nuevo proceso de comunicación.

Hoy, en día *Marshall* [68], científico en computadores (computer scientist), ha manifestado que "*es difícil tener sueños gráficos en un mundo tan ampliamente textual*". Por ello, los nuevas tecnologías de la comunicación electrónica han abierto nuevas posibilidades para

aquellos que sólo se contentaban con la imagen y la palabra, puesto que permiten abrirse a los modelos animados y multi-dimensionales en la comunicación, y por tanto, una nueva lógica y manera de ver la complejidad de las cosas, más allá de la perspectiva lineal con el uso de la geometría que crea una nueva versión sobre la ilusión de profundidad y perspectiva.

d) *El Hipertexto*. Hipertexto es un término acuñado por *Theodor Nelson* [69] , quien lo definió como la extensión textual y escrituraria, no secuencial y ramificada que le permite al lector, acceder en condiciones potenciadas de visualización y consulta a una pantalla interactiva. Popularmente se concibió al hipertexto como una serie de colcha de retazos de textos que se iban agrandando a medida que se conectaban con otros vinculados entre sí, por una especie de eslabones que permitían al lector llegar a diferentes sendas, brechas y locaciones, a través un texto inicial u originario que lo permitía.

---

(68) MARSHALL, Brain. *STOP BIT*. Citado por Ethain Kasth. Ibídem. Sin dirección electrónica.
(69) NELSON, Theodor. *LITERARY MACHINES*, 1981. Citado por el prof. Ethain Kasth. Ibídem. Sin dirección electrónica.

La información contenida en un libro por esencia, esta organizada de forma lineal. Los libros tienen un principio y un fin; vale decir, un especial y caprichoso diseño según el estilo, ánimo y aún la especialidad temática de cada autor. El papel del autor no es solamente el componer el texto, sino presentar una estructura y una "línea"argumental. La Tabla de contenido es el dispositivo que resume la naturaleza de la ruta seguida por el autor. En definitiva es la única posible según su criterio y el del lector que esta sometido a dicho esquema, con limitadas posibilidades, sí aquél decide cambiar o ampliar un tema, subtema o nota de pie de página, siempre por su cuenta y riesgo, pues en esa aventura el timonel lo lleva únicamente el lector.

Ahora bien, el Hipertexto unido a las nuevas tecnologías de la información y comunicación (TIC) que posibilita la emisión y recepción de texto, imágenes gráficas o fotográficas (imágenes digitalizadas) y sonidos se conoce hoy en día como Hipermedia . Por ello, el hipertexto o hipermedia es la información sobre la pantalla, con texto o imagen que se colocan para permitirle al usuario o al lector moverse a través de éste o más allá en una variedad formas o maneras. El usuario, por así decirlo, dispone de nuevas herramientas para navegar a través de la información y usarla de tal forma que antes no era posible hacerlo, o al menos, resultaba embarazoso o engorroso intentar hacerlo con el texto impreso.

El Hipertexto entonces, permite unir información sobre un mismo tema situada en diferentes lugares, siempre que se halle en red, con lo cual la información es más flexible que la información material que tiene "límites" propios de su naturaleza y estructura lineal. El Hipertexto constituye una especie de catalizador de la comunicación impresa y electrónica, pues permite a los usuarios escapar de los esquemas un tanto rígidos, pétreos que en cierta forma

constriñen al lector al acceder a un texto escrito, lineal y encuadernado, a un especie de enclaustramiento predefinido. El Hipertexto por el contrario, permite establecer enlaces o vínculos con varios textos o partes de estos, aún cuando se halle en diferentes lugares o direcciones electrónicas, con lo cual posibilita *unir diversas unidades de texto de manera tal que lo usuarios puedan moverse rápida y oportunamente entre las ideas asociadas entre sí sobre un mismo tema*" [70] .

El hipertexto constituye también una extensión de las capacidades interactivas de los medios de comunicación electrónicos. La interacción implica para el usuario la espera de contestaciones que van más allá de lo solicitado, así como también la capacidad de seleccionar la opción que más le convenga, o igualmente escoger las opciones típicamente disponibles en el texto impreso.

---

(70) MITAL, V. y JOHNSON, L. *ADVANCED INFORMATION SYSTEMS FOR LAWYERS*, 1992.Citado por Ethain Kasth. Ibídem. Sin dirección electrónica.

Con el hipertexto el usuario puede moverse libremente por diferentes textos o partes de estos, en tanto lo posibilite el texto mostrado en pantalla, aún cuando se encuentre geográficamente a sitios muy distantes y en lugares tan recónditos, a velocidades y formatos electrónicos, o también usar la características del texto impreso, tales como ir a las referencias de pie de página o las obras citadas en ellas (información oblicua del texto principal).

Los textos existen en un espacio discreto y se diseñan para ser leídos de una manera lineal: según el número de la página, según la tabla de contenido, o más importante aún, según los índices por materias que le permiten al usuario localizar una información precisa y de mayor interés. El Hipertexto, especialmente constituye un mejor ambiente para el usuario o lector cuanto este conectado a una red con su ordenador, lo cual le permite ir más lejos, reestructurar la lógica tradicional de la impresión (la lógica textual: libro, revista, colección, etc) y trasladarse más allá de lo físico para conseguir la información precisa, oportuna y rápida por medios electróncos.

4.2. CONCEPTUALIZACION DE DOCUMENTO INFORMATICO, ELECTRONICO O TELEMATICO.

La Jurisprudencia, la legislación y la doctrina española han reconocido la existencia de los llamados documentos que genéricamente se han denominado *informáticos*, por referirse a aquellos que son producto de medios informáticos, electrónicos o telemáticos.

En ese género se entienden, en primer término, los documentos almacenados ("storage") en *la memoria* [71] del ordenador, (o también conocida como "memoria central") como los

almacenados en la memoria de algunas unidades periféricas, idóneas para tal actividad electromagnética ("memorias auxiliares"). v.gr. Los "disquetes" o

---

(71) Constituye el ambiente de trabajo del propio computador. Es el lugar donde tiene lugar toda la actividad retrospectiva de la "máquina informática", al igual que si se anotara en una pizarra o tablero, una cierta información que luego se recorta, selecciona, copia, modifica, borra o se utiliza en el momento y circunstancias apropiadas para consulta, cesión, trasmisión, etc. Ello explica, más gráfica, que técnicamente, cuanta memoria necesita un usuario al adquirir un equipo informático de la categoría de los "microcomputadores" o "PC´s"--computer personal-- , pues no se requerirá por ejemplo, una memoria del tamaño de una cancha de fútbol, si la utilidad va a ser como máximo de una mesa de arquitecto. Un abogado, Jefe de un grupo especializado, requerirá como máximo un "PC totalmente cargado", es decir, con 640 Kiloctetos -- "640K" -- de memoria, cuando utilice el equipo en llevar cientos de expedientes, organizados por áreas jurídicas, temas, casos, etc., con índices generales y temáticos; con jurisprudencia, doctrina actualizada; una cierta cartera y facturación de clientes; y por supuesto, esté interconectado con otros ordenadores a través de una línea telefónica y un MODEM (*M*Odulador/*DEM*odulador de señales de comunicación).

discos flexibles, los "hard disk" , los variopintos compac disck, las unidades de "backup", etc . Estos los podríamos llamar "*documentos in*" o dentro de la memoria del ordenador.

En segundo término, los documentos que eventual o definitivamente pueden salir de la memoria hacia el exterior para ser impresos por unidades periféricas, como las impresoras para ordenador de todo tipo y clase, como los "plotters" (impresión gráfica de figuras o planos arquitectónicos en serie o por unidades, mono o multicolor),conocidos como "documentos printout" [72].

Igualmente, aquellos documentos que pueden salir de la memoria del ordenador, a través de las unidades periféricas diferentes a las que imprimen información. Estos documentos los podríamos llamar "*Documentos output*". v.gr. En el monitor o pantalla, en forma única y exclusivamente visual, por recuperación del archivo ("*file*"), el fichero o banco de datos ("*database o personal information bank*") donde se encuentre. Igualmente, en forma auditiva, a través de altoparlantes (documento auditivo); o en forma audio-visual textual o de imágenes o gráfica, por video cámara conectada al ordenador: *documento auditivo-visual*.

Son *documentos output* especiales, los que salen de la memoria del ordenador a través de unidades periféricas que transfieren información entre ordenadores, sin importar la situación locativa, el sitio geográfico o el número de personas receptoras o emisoras (sistemas informáticos *on line*). v.gr. a través de una línea telefónica y un MODEM (entendiendo por tal, la tarjeta electrónica de intercomunicaciones incorporada al ordenador --"*tarjeta-modem*"-- o bien el aparato o dispositivo igualmente electrónico que cumple iguales funciones pero se diferencia de la tarjeta en que es una unidad externa al ordenador) que permite comunicación entre ordenadores, en pantalla en forma textual, (en tiempo real "real-time" e interactivamente: comuni- cación telefónica vía modem textual), en pantalla en forma visual y auditiva (en tiempo real, interactiva, vía modem y con apoyo de una cámara de video conecta al ordenador), o en

pantalla textual, visual y auditiva, con idénticas características y utilización de periféricos auxiliares de éstos. Estos documentos output especiales podrán ser *teletextuales* o *televideo-auditivos*.

Sin embargo, documentos output especiales podrán convertirse en documentos out simplemente, cuando son recuperados para consulta en unidades periféricas

---

(72) DAVARA RODRIGUEZ, Miguel. MANUAL DE DERECHO INFORMATICO. Ed. Aranzadi, Pamplona (Esp), 1997, pág. 350.

diferentes a las que imprimen un documento, es decir, mediante un monitor o pantalla, por ejemplo. Igualmente pueden convertirse en documentos printout, cuando se recuperan o salen de la memoria principal o auxiliar (hard disk o discos flexibles o compactos, etc) para ser impresos mediante un periférico que imprime información digital: impresoras (con sistema de impresión común, láser, o de simulación: sistema burbuja), plotters, etc. O más aún, en documentos in, cuando se almacenan en memoria central o auxiliar de un aparato o dispositivo informático o electromagnético. Esta reversibilidad del documento informático, es quizá la característica esencial e inimitable por cualquier otra forma de documento, incluido el impreso.

4.2.1. DOCUMENTO INFORMÁTICO EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO ESPAÑOL.

No pretendemos agotar el tema, pues sólo el epígrafe sugiere una tema de tesis doctoral. Perseguimos develar el aspecto iusinformático del documento que la jurisprudencia del Tribunal Supremo, ha comenzado a llamar "*informático*" en forma muy genérica. La conceptualización de tales documentos desde ésta visión no tiene en cuenta la rama del derecho a la que es aplicable, como veremos, aunque el área del derecho público ha sido la punta del iceberg de la teorización.

En efecto, el Tribunal Supremo de España, Sala 2ª , en la década de 1990, en sus múltiples decisiones ha reconocido la existencia de los *documentos informáticos*, a partir del concepto de documento impreso, escrito, similar o tradicional (STSS 19/04/91. FJ.4. M.P. Soto Nieto; 14/11/93.FJ.3. M.P. Puerta Luis; y, 3/06/94. FJ.1. M.P. Martín Canivell; entre otras.), o bien aplicando el art. 26 del nuevo C.P.Esp de 1995 (STSS: 10/07/96. FJ.6.M.P: Soto Nieto; 121/1997, y 3/2/97.FJ.2, M.P:Joaquín Delgado García); pero al fin y al cabo, *documento informático* desde el punto de vista del hardware y software.

El Tribunal Supremo viene reconociendo reiteradamente que cada vez se impone, frente a cualquiera otra concepción, un concepto material de documento, el cual desborda cualquier lindero entre el derecho privado y público, cuando menos "en lo concerniente a la sustentación

material del documento privado, puede decirse haberse abierto horizontes inéditos que sobrepasan, con mucho, los hasta ahora conocidos para el documento público. Ya la sentencia de esta Sala de 8 Abr. 1991, apostando por un criterio de amplitud en correspondencia con los medios técnicos hoy impuestos arrolladoramente" [73]. y en los avances de las nuevas tecnologías TIC y la informática

---

(73) Vid. AA.VV. *COMPENDIO DE DISCOS*... SENTENCIA T.S., Sala 2, M. P.: Soto Nieto. Fecha: 10/07/96. F.J. 6

(STSS,19/04/91;14/11/993; 3/06/94; 10/07/96; 11/23/96); y por ello, "documento que ha de constar sobre un soporte material, lo que tradicionalmente ha venido significando por escrito aunque puede ser hoy también, *de acuerdo con los avances técnicos, un diskette, o documento informático*, un film o un vídeo (S de 17 May. 1993)" [74]. Así, "se impone un concepto material de documento, en racional y fundada homologación de los más adelantados y funcionales medios con los sistemas tradicionales imperantes hasta ahora" [75] .

Ha pesado tanto la visión material de documento que se ha enfatizado en la *Validez de impresos y soportes informáticos*, indispensables para cumplir una actividad o función estatal como por ejemplo, la "resolución judicial que autorizó la diligencia de entrada y registro...". La utilización de impresos y de soportes informáticos constituye una exigencia de toda oficina donde ha de despacharse un elevado número de oficios sustancialmente idénticos". Por esto, "procede decir que su carácter de documento impreso -suscrito por la Autoridad judicial- no puede ser considerado causa bastante para privarla de validez y eficacia jurídicas" [76].

> *El concepto de documento, actualmente, no puede reservarse y ceñirse en exclusividad al papel reflejo y receptor por escrito de una declaración humana, desde el momento que nuevas técnicas han multiplicado las ofertas de soportes físicos capaces de corporeizar y dotar de perpetuación al pensamiento y a la declaración de voluntad; una grabación de vídeo, o cinematográfica, un disco o una cinta magnetofónica, los disquetes informáticos, portadores de manifestaciones y acreditamientos, con vocación probatoria, pueden ser susceptibles de manipulaciones falsarias al igual que el documento escrito* [77]

Con la definición de tipo legal de *documento* a los efectos de la norma penal, se recoge expresamente una conceptualización de *documento informático* incorporada en el art. 26 del nuevo C. P. Esp., aprobado por la LO 10/1995 de 23 Nov., como subproducto de los aportes de la doctrina, y sobre todo, de la jurisprudencia. Sin embargo, la labor jurisprudencial, no se detiene ahí y aplicando una hermenéutica acorde con la realidad actual y visionando el futuro cierto que provienen de las tecnologías TIC y la informática, ha interpretando el mentado artículo 26, que dispone: " a los efectos de

(74) Vid. AA.VV. *COMPENDIO DE DISCOS*... SENTENCIA TS. Sala 2, M.P.: Martín Canivell. Fecha: 3/06/94. F.J.1
(75) Vid. AA.VV. *COMPENDIO DE DISCOS*... SENTENCIA. T.S.Sala 2. M.P.: Soto Nieto. Fecha: 19/04/91. F.J.4
(76) Vid. AA.VV. *COMPENDIO DE DISCOS*.. SENTENCIA. T.S. Sala 2, M. P.: Puerta Luis. Fecha 14/11/93. F.J. 3.
(77) Vid. AA.VV. *COMPENDIO DE DISCOS*... SENTENCIA. T.S.Sala 2.M.P.: Soto Nieto. Fecha: 19/04/91. F.J. 4.

este Código se considera *documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*", así:

> *... merecerá la condición de documento cualquier soporte de los hoy conocidos o que en el futuro pudieran concebirse, con tal de que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica. Cual se resalta, lo decisivo será la trascendencia jurídica que pueda derivar de la información proyectada el soporte u objeto material, cuyo sentido o contenido se manipula o altera* [78]

4.2.2. DOCUMENTO INFORMATICO EN LA LEGISLACION ESPAÑOLA. CLASIFICACION DEL DOCUMENTO INFORMATICO.

Por su parte, la Ley 30 de 1992, Ley de Régimen jurídico de las administraciones públicas y del procedimiento administrativo común (LRJPA, antes LPA), al regular las relaciones de los ciudadanos con la Administración General del Estado, destaca la incorporación de las nuevas tecnologías TIC en vida iusadministrativa y, particularmente denota, la "*validez y eficacia de documento original* " a los obtenidos con "*medios electrónicos, informáticos o telemáticos*". Si bien la existencia de éstas modalidades de documento informático se hallan curiosamente desintonizadas con la LORTAD, que regula todo lo atinente a los datos de carácter personal tratados por medios informáticos en un procedimiento de idénticas características tecnológicas, y máxime cuando, se por la misma época: año y fecha, fueron expedidos, con tan solo un mes de diferencia [79]; lo interesante a destacar de esta ley es que no sólo se suministra una conceptualización de lo que se entiende por *documento informático,* sino que además, se propone una clasificación basada, a nuestro juicio, en que el término informático es el género y "electrónico" o "telemático" son las especies, pues parten de un mismo tronco o fundamento: las nuevas tecnologías TIC y la informática, aplicadas al concepto tradicional de documento.

La desconexión entre las dos normas (Ley 30/92, Nov.27 y LO 5/92, Oct.29), es flagrante, pues la LRJPA, en los arts. 37, 38 y 45, regula aspectos propios e *in esencie* de la LORTAD, que esta guarda silencio inexplicablemente. Existe un divorcio normativo de un mismo fenómeno tecnológico propio de la cultura electrónica. En

(78) Vid. AA.VV. *COMPENDIO DE DISCOS...* SENTENCIA T.S., Sala 2, M. P.: Soto Nieto. Fecha: 10/07/96 F.J. 6
(79) GONZALEZ NAVARRO, Francisco. *COMENTARIOS A LA LEY DE REGIMEN...* Ob.cit., pág. 691

efecto, es apenas obvio que datos de carácter personal y familiar pueden encontrarse en ficheros o bancos de datos, en archivos o registros (de cualquier naturaleza); y sobre todo, en *documentos*, como producto de creación, ingresos o accesos y transferencias (cesión o consulta) por medios informáticos, electrónicos o telemáticos, que por regla general terminan además, constituyendo documentos informáticos o electrónicos o telemáticos.

Por esto, el art. 37 LRJPA, al regular el Derecho de acceso a archivos y registros, dispone: "1. Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud".

No nos interesa destacar, por el momento en este trabajo el aspecto iusadministrativista de la norma, profusamente explicado por los especialistas (v.gr. *González Navarro*), sino el ámbito iusinformático; es decir, poner el énfasis en que un procedimiento realizados por medios informáticos, electrónicos o telemáticos, tendrá todas las garantías, derechos, limitaciones, etc., que se prodigan para todo ciudadano. Uno de ellos, quizá el más importante e integrante del habeas data es el derecho de acceso a los registros o documentos que le conciernen. Se reconoce así que en un documento es continente y contenido de datos de carácter personal, analizados a la luz de la LORTAD. Máxime, cuando se reconoce que no sólo se puede acceder a un registro o un documento escrito o tradicional, sino también a cualquiera que tenga diversa forma de expresión de éste (o sea, gráfica, sonora o imagen), o tipo de soporte material (papel, discos de hardware o software, cintas de backup, video, etc).

Se reconoce el derecho de acceso a documentos productos de la tecnología TIC y la informática, tanto en la forma como en la clase de soporte que los contiene, al hacer mención a la información de cualquier tipo no sólo escrituraria o alfanumérica, sino también información digital: gráfica, sonora e imagen (elementos indispensables para configurar un documento de la tecnología de la multimedia y del hipertexto).

Por su parte, el art. 37-2, LRJPA, confirma lo anterior y concreta el derecho de acceso a "los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuren incompleto, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del

tiempo..." . Esta norma completa las facultades inherentes al derecho de habeas data (actualización y rectificación de datos) y hace más evidente la conexión de esta norma con la LORTAD, a fin de entender la significancia de que son datos de carácter personal referidas a los documentos que los puedan contener.

El art. 38 LRJPA, a nuestros efectos, hace referencia, a la informatización de los registros de entrada y salida de documentos que deben observar las administraciones públicas del Estado, pero particularmente nos interesa destacar que la nueva ley observando los avances tecnológicos TIC y la informática, prevé la incorporación de sistemas informáticos de constancia y registro de todo cuanta información se produzca por personas naturales, jurídicas, institucionales o del Estado. Se hace énfasis en el *soporte informático,* (elementos de hardware y software), diferentes al tradicional o conocido soporte documental escrito (v.gr. Libros de registro, constancia, etc.)

El art. 45 LRJPA, Sobre la incorporación de medios técnicos al ámbito iusadministrativo, hace referencia exclusiva al empleo y aplicación de las técnicas, programas, aplicaciones y medios electrónicos, informáticos y telemáticos por parte de las Administraciones Públicas, "*para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las leyes*" (45-1). Igualmente, establece una clasificación de los documentos, atendiendo a su forma de emisión, a los soportes utilizados y a "los medios electrónicos, informáticos o telemáticos" empleados y a la manera de ser "almacenados" por medios electrónicos, informáticos o telemáticos. En todo caso, estas clases de documentos, formas, características y funciones "*gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por esta u otras leyes*" (45-5).

Las razones de sintonización, además de la parte temática y a nuestros efectos, entre la LRJPA y la LORTAD, vienen dadas por la práctica legislativa prevista en las normas de desarrollo o de carácter reglamentario de la LRJPA. Estas normas regulan el fenómeno tecnológico TIC, la informática y el documento. En efecto, el Real Decreto (R.D).núm. 263/1996, Feb.16., reglamenta la utilización de técnicas electrónicas, informáticas y telemáticas por parte de la Administración General del Estado, al desarrollar el art. 45.5 de la LRJPA, que constituye una "*verdadera piedra angular del proceso de incorporación y validación de dichas técnicas en la producción jurídica de la Administración pública así como en sus relaciones con los ciudadanos"* (Exposición de motivos --E.M.-- R.D.263/1996); y, suministra un catálogo de definiciones técnicas aplicables al campo del derecho en todo lo atinente al documento informático, electrónico o telemático.

Uno de los aspectos capitales que destaca la E.M., del R.D. 263/1996, es el referido a los "*problemas de la emisión, copia y almacenamiento de los "documentos automatizados", desde una óptica que persigue --con las necesarias cautelas y garantías-- otorgar a dichos documentos idéntica validez y eficacia que a los comúnmente reconocidos y aceptados: los documentos en soporte de papel"*. En los artículos 6 a 8 del R.D., mentado se abordan estos problemas en concordancia con lo estipulado en la LRJPA y la LORTAD, que aquí se menciona expresamente en el art.8.

Documento, según este R.D., citado se considera toda "*entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada"*. (art. 3-d). En esta definición se hallan inmersas las características y funciones de los documentos informáticos, electrónicos y telemáticos, que antes hemos analizado. Sólo con éste tipo de documentos es posible almacenar, editar, extraer o transferir datos o informaciones de tipo digital (textual, imagen o auditiva). Por esto, el R.D., en el articulado siguiente describe pormenorizadamente las características y funciones de esta clase especial de documentos devenidos de la tecnología TIC y la informática.

La emisión de documentos y copias que hayan sido producidos por medios electrónicos, informáticos y telemáticos en soportes de cualquier naturaleza ("sobre el cual es posible grabar y recuperar datos", art.3-a R.D.263/1996) serán válidos siempre que quede acreditada su integridad, conservación y la identidad del autor, así como la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación (art.6-1 Ibídem).

Las copias de los documentos originales almacenados por medios o soportes electrónicos, informáticos o telemáticos, tendrán la misma validez y eficacia del documento original siempre que quede garantizada su autenticidad, integridad y conservación (art. 6-2 Ibídem).

Los documentos electrónicos o telemáticos que se concretan básicamente en la comunicación en soportes o a través de medios o aplicaciones informáticas, electrónicas o telemáticas y serán válidas siempre que: a) Exista constancia de la trasmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones, b) se identifique fidedignamente al remitente y al destinatario de la comunicación, c) en los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos haya señalado el soporte, medio o aplicación como preferente para sus comunicaciones con la Administración en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa (art.7-2 Ibídem).

Podrán almacenarse por medios o soportes electrónicos, informáticos o telemáticos todos los documentos que contengan "actos administrativos" que afecten a derechos o intereses de los particulares. Igualmente podrán conservarse en soportes de idéntica naturaleza en la cual han sido producidos, así como en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo (art. 8-1 y 8-2 Ibídem).

El derecho de acceso a los documentos almacenados por medios o soportes electrónicos, informáticos o telemáticos, se regirá por lo dispuesto en la LRJPA, art. 37, o en su caso, por la LORTAD, así como en sus normas de desarrollo.

Otros cuerpos normativos del derecho español, hacen referencia a los documentos informáticos, electrónicos o telemáticos: unos, para brindar la suficiente tutela o garantía de *última ratio*, como el C.P.Esp., de 1995, que utiliza una terminología propia de la cultura electrónica y aplicable al caso *sub examine*. v.gr. El art. 197.1, *ab initio*, tipifica el delito de "apoderamiento de papeles, cartas, *mensaje de correo electrónico o cualesquiera otros documentos* o efectos personales". Considerando a los "mensajes de correo electrónico" como una especie de documentos informáticos, tal como se precisará más adelante. En el art.197-2, expresamente se hace alusión a los "*ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo...*". Existen otros textos normativos penales que intencionalmente dejamos de tratarlos por no servir a los propósitos de la Parte IV de este trabajo, pero que, en todo caso, sí confirman la parte legislativa del fenómeno TIC y la iusinformática. v.gr. Art. 390 sobre falsedades documentales devenidas de los despachos transmitidos por los servicios de telecomunicaciones en los que se incluya un medio informático, electrónico o telemático. Piénsese en el FAX-MODEM enviado de computador (empresa de telecomunicación) a computador personal. Es un típico documento telemático ("Documento in" en memoria, o output en pantalla, según el momento de almacenamiento o recuperación) con posibilidad de salida de información impresa, fuera del sistema ("Documento Printout"). Fax en el que se utiliza software y hardware y no un aparato eléctrico o fax corriente. Otros, cuerpos normativos, que aisladamente regulan aspectos y documentos electrónicos, y que más adelante comentaremos v.gr. Ley 28 de diciembre de 1992, sobre el IVA, arts. 88.2 y el R.D. 2402, 29 de diciembre de 1992, art. 4, sobre transacciones electrónicas --EDI-- de carácter administrativo.

4.2.3. LA DOCTRINA SOBRE EL DOCUMENTO INFORMATICO, ELECTRONICO O TELEMATICO.

El profesor *Davara* [80], prefiere hablar de "*documento informático"*, en tres aspectos: a) la información en soporte de papel generada por medios informáticos. v.gr. el listado impreso de la información que se encuentra en un soporte informático. Es el documento "*printout"*; b) el documento informático que se encuentra en un soporte de información electrónico, creado por datos almacenados en la memoria de un ordenador. Es el documento "*input"*; y c) el soporte de información electrónico formado mediante el intercambio de mensajes con estructura determinada utilizando unas normas de intercambio informáticas, conocido como EDI (*Electronic Data Interchange*).

La clasificación se basa en el tipo de soporte en el que aparecen los documentos, pues mientras la clasificación a, y b, según el autor, son en papel, y los documentos EDI, tienen un soporte informático. Sin embargo, como vimos anteriormente todos los documentos creados, almacenados, editados, recuperados o transferidos se realizan por medios informáticos, electrónicos o telemáticos, y como tal, el procedimiento, funciones, características son de igual naturaleza para que se reputen como tales, de lo contrario, serán documentos escritos o impresos. Situación diferente es que, de conformidad con la característica *sine qua nom* de esta clase de documentos considerados genéricamente informáticos, es decir, *la reversibilidad de los mismos,* por la cual se pueden convertirse en documentos "in", "output" o "printout", según las circunstancia y forma de recuperación del documento, pero originalmente son informáticos y serán electrónicos o telemáticos si utilizan medios electromágneticos y eléctricos para transferir entre ordenadores, para almacenar o recuperar información. No es el resultado final del proceso informático lo que determina la clase de documento, sino el empleo de medios informáticos, electrónicos o telemáticos en todo el procedimiento, y más aún la determinación de cada fase o etapa lo que clasifica cada tipo de documento informático genéricamente hablando. Pues de lo contrario todos los

(80) DAVARA R. M. *MANUAL DE DERECHO INFORMATICO*.... Ob. cit., pág. 350.

documentos, sin excepción terminarían siendo escritos y en un soporte de papel, siempre que se trate de texto, imágenes fijas, gráficos, o impresos en cintas de video o de sonido, si se trata de información digital auditiva o de imágenes en movimiento.

El profesor *González Navarrro* [81], siguiendo a *Davara* para desentrañar el significado de los significantes "documentos electrónico, informático y telemáticos", utilizados por el art. 45 LRJPA, sostiene:

a) Documento electrónico. Es el mensaje reproducido en soporte papel en escritura tradicional pero que contiene una información generada o tratada informáticamente. La versión a signos de la escritura convencional de la información codificada en un disco informático, sería un documento en sentido estricto, ya que puede ser incorporado a un expediente, y autenticado incluso con la firma convencional.

b) Documento informático. Es el mismo anteriormente aludido: soporte de papel continente de información generada por un ordenador. Es el documento "printout". Puede ser autenticado mediante símbolos y signos tradicionales. Se le llama también "input", no porque sean datos que entren al ordenador, sino porque son el resultado de un proceso informático que ha permitido elaborar su contenido.

c) Documento telemático. Un soporte de información mediante intercambio de mensajes. v.gr. Documento EDI.

Los juristas *Maronda F.,y Tena F.* [82], hacen un amplio catálogo de definiciones de documento desde el punto de vista del derecho común: unas, a favor de la consideración como documentos a los obtenidos por medio de soportes informáticos, electrónicos o telemáticos; y otros, en contra de dicha postura. Sin embargo, perdura en sus argumentos los que sostienen la primera hipótesis y a nuestros efectos, resaltamos los siguientes:

Siguiendo a *Rocco Bogini* [83], entiende que *documento electrónico* ofrece los

---

(81) GONZALEZ N. F., Ob. cit. págs. 819-820

(82) MARONDA FRUTOS, Juan y TENA FRANCO, M˜., Isabel. *LA INFORMATICA JURIDICA Y EL DERECHO DE LA INFORMATICA.* En: Revista General del Derecho. R.G.D. Año III, núm. 630, Marzo, Valencia, 1997, pág.1755-1759

(83) Citado por MARONDA FRUTOS, Juan y TENA FRANCO, M˜., Isabel. *LA INFORMATICA JURIDICA Ob*. cit., pág. 1756.

tres requisitos fundamentales de todo documento en papel: la legalidad, la inalterabilidad y el reconocimiento.

Rovanet, J. [84], considera que la electrónica debe ser considera escritura a todos los efectos y por lo tanto engloba el documento electrónico en la categoría de los documentos en sentido jurídico.

En definitiva, considera que el documento es un soporte material al que se lo ha impreso, por medios electromagnéticos, un pensamiento con un determinado significado. La única

diferencia con el clásico documento escrito estriba en que la impresión se ha hecho en un lenguaje especial, distinto al común (se refiere al lenguaje de no natural o utilizado por los ordenadores, a veces conocido como "lenguaje de máquina"). Aquí se rebate el hecho de que todo documento tiene como elemento esencial la firma autógrafa u ológrafa, según la legislación española. Sin embargo, el propio *Rovanet*, obvia ese requisito esencial, diciendo que la firma autógrafa no es la única manera de signar y que sabiendo que la firma es un "*trazado gráfico*", existen otros mecanismos que sin ser firma autógrafa, son trazados gráficos que suministran autoría y obligan a sus signatarios, tales como las claves, códigos, signos y sellos. Más aún, pueden existir documentos comunes que carecen de firma autógrafa, al igual que documentos electrónicos, y no por ello, unos y otros desvirtúan su naturaleza de documentos. En el caso, del documento electrónico la firma autógrafa o equivalente puede sustituirse por la criptografía, por medio de cifras, signos, códigos o claves que permiten asegurar su procedencia y veracidad [85].

4.3. EL DOCUMENTO "EDI" (*ELECTRONIC DATA INTERCHANGE*)

El *nomen juris* subsiguiente a *documento*, varia en la medida que el recipiente o continente sea por medios escritos o no escritos, pues al fin y al cabo, el concepto de *documento*, es uno sólo sea cual fuere el soporte en el que se halle, o el área del derecho en la que se suministre. La especie de apellido impuesto al documento (v.gr. documento *informático, electrónico o telemático*), sólo viene en función de la distinción del soporte en el cual se halla almacenada, registrada, editada o recuperada la información; así como de los medios informáticos físicos o lógicos empleados, tal como vimos al analizar el art. 3-d, R.D. Núm.263, Feb.16/1996, sobre utilización de medios, soportes, aplicaciones informáticas, electrónicas o telemáticas por parte de la Administra

---

(85) Ibídem., pág. 1756

ción del Estado. Sólo así, es entendible la clasificación de documento desde el punto de vista iusinformático en informáticos, electrónicos o telemáticos, válido para cualquier rama del derecho donde se estudie, aplique o analicen.

El documento electrónico de más amplia circulación, cobertura e importancia en la iusinformática, es el denominado EDI o *Electronic Data Interchange*. En versión castallena IED: Intercambio electrónico de datos.

Por IED, entendemos el intercambio de datos o mensajes en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o financieras,

administrativas e incluso entre personas naturales o jurídicas privadas, y sobre todo, públicas. Aunque, su origen haya sido en las órbitas del derecho crematístico, hoy en día cubre una amplia zona del derecho público

Para esta estructura de intercambio de datos o mensajes o EDI, cumpla sus fines y propósitos, debe necesariamente disponerse de un sistema informático de hardware y software idóneo previamente instalado y en funcionamiento. Sin embargo, en líneas generales un sistema de este tipo ha de cumplir tres requisitos básicos: a) el intercambio se ha de realizar por medios electrónicos o telemáticos, b) el formato tiene que estar normalizado, según el ordenamiento jurídico de los Estados involucrados en la transacción, [86] y c) la conexión ha de ser de ordenador a ordenador [87]. Es decir, que

---

(86) "Normalización y homologación. Es lógico que la conservación de estos documentos tenga que hacerse de acuerdo con unas normas que faciliten, en una posible comprobación, la veracidad de su contenido y la fiabilidad de la información, así como una sistematización y orden en su organización y adecuación y conocimiento de las operaciones o procesos a los que han podido ser sometidos informáticamente. Se tendrían que acometer unas especificaciones que tuvieran como objeto establecer ciertos criterios unificados que permitieran garantizar el contenido de un documento. Esto es, acudir a actividades típicas de normalización, establecidas por la administración, para poder garantizar la autenticidad de los documentos informáticos respecto a su contenido. De otra parte, se establecerían unos procedimientos de archivo, identificación y transcripción de los documentos informáticos, para poder acceder a la acreditación de sus contenidos mediante un instrumento fiable; como es lógico, estas funciones de homologación de procedimiento estarían encomendadas a la Administración. Estas tareas de normalización y homologación, establecidas de acuerdo a unos criterios objetivos --armonizados en el seno de la Comunidad Europea-- garantizarán los contenidos de los documentos informáticos, abriendo el camino, junto con otros pasos a recorrer -- como el de la firma electrónica-- para que puedan, incluso, ser considerados como documentos públicos, cumpliendo los requisitos que, a ese fin, se establezcan. De acuerdo con ello, se realizará el almacenamiento informático -- con unas instrucciones redactadas y archivadas-- durante todo el tiempo que se tenga el soporte informático con los datos almacenados y se protegerán contra cualquier alteración y describirán las operaciones a las que han podido ser sometidos; *así, se garantiza la veracidad, la seguridad, confidencialidad y conservación de la información en ellos contenidos.* Todo ello proporcionará una seguridad respecto a la originalidad del contenido, con la misma fiabilidad --si no más-- de un documento público". Cfr. DAVARA RODRIGUEZ, M. *MANUAL DE DERECHO*... Ob. cit., pág. 360

(87) Vid. CAVANILLAS MUGICA, Santiago. *INTRODUCCION AL TRATAMIENTO JURIDICO DE LA CONTRATACION POR MEDIOS ELECTRONICOS (EDI)*. En: Revista Actualidad Aranzadi, Ed. Aranzadi, Núm. 10, Enero 1994, Pamplona, pág.1 y ss.

la intercomunicación es eminentemente mediante las nuevas tecnologías TIC y la informática, no humana.

Existen diferentes tipos de intercambio electrónico de datos en el actual tráfico global de documentos, por ello, *ab priori*, se han clasificado en: a) Intercambio electrónico de datos (IED), b) transferencia electrónica de fondos (TEF), c) la contratación electrónica [88], y d) los mensajes de correo electrónico [89]. En el presente estudio, y a nuestros efectos haremos referencia al EDI y el E-Mail o correo electrónico.

Algunas de las razones que justifican la implantación de los documentos EDI, son: a) Precisión. Los datos intercambiados entre sistemas informáticos son más exactos que los que se

introducen manualmente; b) Velocidad. Los datos procesados por el ordenador circulan más rápidamente a través de las redes que cuando hay intervención manual; c) Ahorro. Se produce un ahorro inmediato en mano de obra, franqueo, copia de archivo y toma de datos; d) Beneficios tangibles. Reducción de existencias, acortamiento del plazo y liberación de espacio de almacenamiento; y, e) Satisfacción del cliente. Cumplimiento del plazo de entregas, mejora en el despacho de aduanas [90].

4.3.1. ESTRUCTURACIÓN TÉCNICA (SOFTWARE Y HARDWARE) Y JURÍDICA.

Para que se cumpla el intercambio electrónico de datos entre los usuarios de un sistema EDI (empresarios [91], funcionarios estatales, particulares) se debe disponer; entre otros requisitos, con un equipo y dispositivos de *hardware* idóneos, tales como: a) Un Ordenador con sus correspondientes unidades centrales y periféricas de procesa miento, almacenamiento, edición, consulta, cesión, trasmisión y recuperación de información o datos; b) Un *MODEM* (Modulador/DEModulador de señales de comunicación), bien sea incorporado al equipo computacional a manera de "tarjeta-MO-

---

(88) Ibídem, pág. 199 .
(89) Ibídem, pág. 199.
(90) Ibídem, pág. 199.
(91) "Si los usuarios del sistema EDI, son dos empresarios que intercambian mensajes electrónicos portadores de cualquiera de las declaraciones, de voluntad o de ciencia, que se producen en la conclusión y ejecución de un contrato: la invitación a la oferta, la oferta, la aceptación, la factura, la receptación de la mercancía y del precio, la denuncia de defectos, etc." CAVANILLAS MUGICA, Santiago. *INTRODUCCION AL TRATAMIENTO*.... Ob. cit., pág. 1.

DEM" , o bien como dispositivo externo al ordenador; c) Una línea telefónica conectada al ordenador vía *MODEM* o por tarjeta electrónica. Esta proporciona además, el servicio de interconexión entre computadores; y, d) Una red específica para transmitir datos o informaciones --R.D.S.I-- (Red Digital de Servicios Integrados).

Una reciente propuesta de Directiva Comunitaria, a propósito del RDSI y a nuestros efectos 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, pretende garantizar la libre circulación de los datos y de los servicios y equipos de telecomunicaciones en la Comunidad mediante la armonización del nivel de protección del tratamiento de los datos personales en el sector de las telecomunicaciones y de

los legítimos intereses de los abonados a los servicios públicos de telecomunicación que sean personas jurídicas. La Directiva especificará, para el sector de las telecomunicaciones, las normas generales establecidas por la Directiva general sobre el tratamiento de datos personales y potenciará la protección de la intimidad de las personas y de los legítimos intereses de los abonados a los servicios de telecomunicación que sean personas jurídicas [92] .

Igualmente se debe disponer de un dispositivo de *software o* programa de computador idóneo para la trasmisión de datos entre equipos computacionales. Este programa o "aplicación informática" debe ser capaz de todas las facultades inherentes a un programa, pero principalmente, emitir y recepcionar información. Los usuarios del sistema tendrán como elementos auxiliares de la labor un "Manual de Usuario del Software" que le sirva además de factor objetivo de homologación y normalización de las actividades entre usuarios.

Entre los elementos de estructuración jurídica, se debe contar con lo siguiente:

a) Unos acuerdos de intercambio entres los participantes en los que se establecen las reglas jurídicas y técnicas que han de regir la comunicación entre los empresarios. Los acuerdos pueden ser bilaterales o plurilaterales, según fueren dos o más los usuarios involucrados en el sistema. En el convenio se regulará, si fuere del caso, la participación

---

(92) En: Comisión de las Comunidades Europeas. Bruselas. 05.03.1997. Abril 11 de 1997, págs. 1-11.

de un intermediario electrónico, llamado "Centro de compensación" [93], o mediante contratos independientes con cada uno de los usuarios [94]; y, b) Facultativamente se puede disponer de un "Centro de compensación", o mejor conjunto de ordenadores que como una especie de oficina postal, con apartados de tipo electrónico hace las veces de "*intermediario* (tercero) *electrónico*", entre los usuarios para que gestione el tráfico informático: almacenamiento temporal, tipo "buzón electrónico" o emisión-recepción de datos o mensajes electrónicos con medidas y procedimientos de alta seguridad (Integridad, autentificación, confiabilidad, no repudio de origen/destino, pruebas de auditoría, pruebas de propiedad, sellos de fechas, *anonimato*) [95]. Este Centro puede ofrecer otras prestaciones, denominadas de "Servicios de Valor Añadido", como *Notaría Electrónica* [96] almacenamiento temporal de los mensajes para cubrir los riesgos de error o pérdida de los mismos, mantenimiento de buzones electrónicos, etc[97]

---

(93) " El Centro de compensación es el núcleo alrededor del cual funciona un servicio EDI. Se trata de un ordenador o conjunto de ordenadores gestionados y operados por un mismo organismo o empresa que proporciona todo el servicio. Tiene las siguientes características: a) Una gran versatilidad y capacidad de comunicación de forma que sea fácilmente accesible a través de un gran número de protocolos diferentes, b) Es el responsable, mediante un sistema de buzones electrónicos, de asegurar la recepción y entrega de documentos entre los usuarios del servicio, c) Debe ser un sistema altamente fiable (hardware y software), d) Sistemas EDI. Su disponibilidad temporal para el usuario es continua, es decir, en cualquier momento del día el usuario puede hacer un envío o recepción de documentos".DEL PESO NAVARRO, Emilio. *Resolución... Ob*.cit. Pág. 215 y ss.

(94) Vid. CAVANILLAS MUGICA, Santiago. *INTRODUCCION AL TRATAMIENTO*.... Ob. cit., pág. 1.

(95) Estos Centros permiten complementariamente "la introducción del concepto de tercera parte confiable que engloba dos aspectos importantes: servicios de soporte, facilitados por los operadores de redes públicas de valor añadido y los servicios de notaría que comprenderían los posibles aspectos legales y que deberían ser prestados por las entidades o profesionales con capacidad legal para ello". DEL PESO NAVARRO, Emilio. *Resolución... Ob*.cit. Pág. 215 y ss.

(96) Notario Electrónico o (Trusted Third Party), que cumpla varias funciones de "tercero" diferente a los centros de compensación; entre otras, la de almacenar los mensajes cruzados entre los usuarios y pueda certificar sobre emisor, receptor, fecha y contenido. Puede realizar actividades de gestión, como "Autoridad de Certificación", de un sistema criptográfico, así se puede obtener niveles de fiabilidad incluso superiores a los del documento escrito; el empleo de un sistema de clave asimétrica, por ejemplo, permitiría que cada documento fuera cifrado ("encriptado") con una clave secreta y personal del emisor, de tal forma que el destinatario pudiera obtener el texto mediante la utilización de otra clave, esta vez pública, del mismo emisor. Vid. CAVANILLAS MUGICA, Santiago. *INTRODUCCION AL TRATAMIENTO*.... Ob. cit., pág. 2 "La firma digital es un tema de vital importancia para el desarrollo de la contratación electrónica", y en general de todo documento electrónico que la requiera. Por ello, quienes sostiene la necesariedad de la firma en todo documento electrónico es indispensable la figura del Notario electrónico que "de forma parecida a como el fedatario público da fe de la autenticidad de un documento gracias a la firma manuscrita, el fedatario electrónico ha de ser capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicaciones". Esta es un labor titánica que se le impone a un ser humano dentro de un sistema que es eminentemente electrónico, en formato y velocidades igualmente electrónicas. Pareciera que queremos aplicar la lógica humana a la lógica electrónica, esto será más difícil, cuanto más complejas sean las tecnologías TIC y la informática. DEL PESO NAVARRO, Emilio. *Resolución... Ob*.cit. Pág. 225.

(97) CAVANILLAS MUGICA, Santiago. *INTRODUCCION AL TRATAMIENTO*.... Ob. cit., pág. 2.

4.3.2. LOS DOCUMENTOS EDI COMO MEDIOS DE TRANSMISION E INTERCAMBIO DE DATOS PERSONALES.

Uno de los aspectos capitales en el Intercambio electrónico de datos (EDI), y más cuando los documentos contienen o son continentes de datos de carácter personal y familiar, es el tema de la seguridad en la emisión y en la recepción de los datos o informaciones, pues como hemos visto **[9 8]**, por definición los sistemas y los proce- dimientos informáticos que utilizan medios electrónicos o telemáticos llevan inmersos las características de seguridad, confiabilidad (de forma y tiempo), integridad, autenticidad; entre muchas otras propias de las nuevas tecnologías TIC y la Informática.

Sin embargo, la normativa jurídica, más que la implementación y estructuración técnica del sistema EDI, han incorporado mecanismos y procedimientos para confirmar, complementar o auxiliar la seguridad en la trasmisión de "flujos" **[9 9]** datos persona-les. Algunos de estos instrumentos jurídicos básicos de *prima ratio* y de ámbito en el derecho Español, son: a) Los

Estatutos Comunitarios relativos al tratamiento de datos por medios informáticos, electrónicos o telemáticos; y, b) LORTAD (LO 5/1992, Oct. 29).

Desde la expedición del Convenio de Estrasburgo de 1981, la Comunidad Europea cuenta con unos instrumentos jurídicos para la protección del intercambio electrónico de datos personales, que en su tiempo se denominó "flujo transfronterizo de datos", para la trasmisión de datos personales "*por cualquier medio*" incluido, por su

---

(98) "Un definición válida de seguridad de la información de seguridad de la información podría ser que es el conjunto de sistemas y procedimientos que garantizan, la confiabilidad, la integridad y la disponibilidad de la información. Estas son las tres características que definen lo que es seguridad de la información. DEL PESO NAVARRO, Emilio. *LA SEGURIDAD DE LA INFORMACION*. En: Revista Actualidad Aranzadi. Núm. 26 de Enero, Pamplona, 1998, pág. 1 y ss.

(99) El Profesor POULLET, define a los flujos "como la trasmisión personal o de las informaciones a través de las fronteras políticas y culturales, por el procedimiento de aprovisionamiento en las filas de computadores", y señala que el intercambio de datos es vital entre las Oficinas de la Información, no únicamente por el aporte en el crecimiento internacional de la producción, sino por cuanto facilita la competitividad y la no discriminación. Además, es necesario reconocer la interdependencia entre oficinas que tienen incorporada en sus estructuras informatización de los datos. La importancia de la internacionalización de datos se refuerza por el aumento de los ficheros informatizados y la progresión rápida y sorprendente de las tecnologías. POULLET Y, en *PRIVACY PROTECTION AND TRANSBORDER DATA FLOW; RECENT LEGAL ISSUES IN ADVANCED TOPICS O LAW AND INFORMATION TECHNOLOGY, COMPUTER LAW SERIES*. Citado por VAN DER MENSBRUGGHE, Patricia. *FLUJOS TRANSFRONTERIZOS DE DATOS EN LA DIRECTIVA 95//46 DE LAS COMUNIDADES EUROPEAS.* En: Revista Actualidad informática Aranzadi. Núm. 20, Julio, Pamplona, 1996, pág. 3 y ss.

puesto, los informáticos, electrónicos o telemáticos. Se valida la aplicación del derecho interno a las transmisiones de datos entre los Estados componentes de la UE, al tiempo que se dan los lineamientos y parámetros generales para hacerlo conforme al Convenio 108. En efecto, se sostiene que un Estado no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte (art. 12-2). Sin embargo, cualquier Estado tendrá la facultad de establecer una excepciones, así: 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 de la otra Parte establezca una protección equivalente; y, b) cuando la trasmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo. (Art. 12-3).

En su momento la República Federal Alemana, propuso una reserva a la aplicación de la excepción b), del art. 12, pues se dijo que se deje a las partes la libertad de estimar, en el cuadro

de su derecho interno en materia de protección de datos, las normas prohibiendo en ciertos casos particulares la trasmisión de datos de carácter personal a fin de tener en cuenta los intereses de la persona afectada dignos de ser protegidos.

Por su parte, la Directiva 95/46/CE, relativa al procesamiento de datos personales por medios informáticos, electrónicos y telemáticos, establece una serie de instrumentos, mecanismos, principios y procedimientos socio-jurídicos para que aseguren el tráfico transfronterizo de datos de personales, considerando precisamente, que la integración de la Unión Europea, va a implicar necesariamente un aumento no- table de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior (C.5).

Así mismo, hace énfasis en las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la trasmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros (C. 7).

Con respecto a la transferencia de datos personales con terceros países que garanticen un nivel de protección adecuado, establece que debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias o datos a transferir (C. 56). Debe existir un proporcionalidad entre las medidas de seguridad de los Estados involucrados en la trasmisión (Emisión/Recepción) de datos personales.

La *telemática* --"*reunión de la informática y las telecomunicaciones*"-- ha propuesto un interesante debate debido a la reglamentación que se ha ido estableciendo respecto de la protección de los datos de las personas tratados en ficheros y a la libre circulación de datos. Las

reglamentaciones internacionales han ido progresivamente encontrando un justo equilibrio entre dos derechos. De una parte se refieren a la protección de las personas físicas; es decir, se protege un interés individual, el *derecho a la intimidad* que tienen los particulares. De otra parte, se refieren al interés colectivo que representa la protección social de la libre información; es decir, el tener acceso a los datos de los individuos. Circulación de información que significa al mismo tiempo la promoción del mercado que contribuye al progreso económico y social, al desarrollo de los intercambios y al bienestar de los individuos [100].

Las razones que justifican la protección de los datos personales son múltiples, sin embargo, se destacan: a) La evolución rápida de las tecnologías TIC y la manera como la informática se integra en la gestión de la Administración e incluso en la de los particulares, b) El crecimiento geomético de los ficheros o bancos de datos en las socie-

---

(100) Ibídem., pág. 3

dades de la informática, en todos los sectores de la vida pública y privada, como mecanismos idóneos, contemporáneos y electrónicos de almacenar, conservar, editar y transferir datos personales o de cualquier tipo; frente a aumento matemático de las medidas de protección y seguridad de los datos en las transmisiones transfronterizas por parte de los Estados e incluso por los mismos particulares; y c) El continuo, permanente e irresoluto conflicto entre derechos fundamentales, libertades públicas e intereses legítimos inmersos en una trasmisión o flujo de datos personales en ámbitos nacionales e internacionales.

La LORTAD, en el ámbito hispano, establece una serie de mecanismos jurídicos para la protección de toda clase de datos personales, la refuerza en el caso de los denominados “datos sensibles” y la hipergarantía en los “datos hipersensibles” (arts.4 a 11). La regla general, de protección al “movimiento internacional de datos”, es la siguiente: No se podrán realizar transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dichos tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la LORTAD, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas (art. 32) .

No se aplicará esto, a título de excepción: a) cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte

España, b) cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional, c) cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos; y , d) cuando se refiere a transferencias dinerarias conforme a su legislación específica (art. 33).

Como lo exalta la E.de M., de la LORTAD, sobre la trasmisión de datos personales, 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.

Estas normas futuras, que hoy son una realidad, son la Directiva 95/46/CE y la propuesta del Consejo y parlamento Europeo, de Marzo 5 de 1997, analizada en el aparte anterior y la propuesta común (CE) del Parlamento y Consejo Europeo, N□ 57/96, aprobada por el Consejo el 12 de septiembre de 1996, 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" **[101]** . Esta propuesta de Directiva es complementaria y de aplicación extensiva de la Directiva 95/46/CE (sobre obligaciones, derechos, limitaciones y medidas de seguridad de datos personales y sobre recursos, responsabilidades y sanciones; entre otros aspectos), pero especializada en la transferencia de datos personales por las nuevas tecnologías TIC con el auxilio de la informática, pues el Parlamento y el Consejo son conscientes que están apareciendo en la Comunidad Europea nuevas redes digitales públicas **[102]**, 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 telecomunicación**[103]**; 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). Así mismo, que las redes públicas de telecomunicaciones deben elaborarse disposiciones legales,

---

(101) AA.VV. *DIARIO OFICIAL DE LAS COMUNIDADES EUROPEAS*. No. C-315, 39□ Año, 24 de Octubre de 1996, pág. 1 y ss.

(102) *Red pública de telecomunicaciones*. "Sistemas de trasmisión, a través de equipos de conmutación y otros recursos que permiten la trasmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicaciones" (Art. 2-c Propuesta Común)

(103) *Servicio de telecomunicaciones*. "Un servicio cuya prestación consiste total o parcialmente en la trasmisión y envío de señales a través de redes de telecomunicación, excepción hecha de la radiodifusión sonora y de televisión". (Art.2-d, Ibídem).

reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a los riesgos crecientes derivados del almacenamiento y tratamiento informático de los datos relativos a los abonados [104] y a los usuarios [105] (C.6).

4.3.3. ALGUNOS DISPOSITIVOS ELECTRÓNICOS DE TRASMISION DE DATOS PERSONALES

Sin que sea una relación taxativa de los dispositivos electrónicos de software de trasmisión de datos personales, actualmente existentes, haremos breves comentarios de los que más se utilizan en las relaciones del ser humano y de éstos con las autoridades estatales de todo nivel y categoría. Todos tienen de común que utilizan medios informáticos, electrónicos o telemáticos para cumplir con sus fines y propósitos; sirven para transmitir uno, dos o grandes cantidades de mensajes a velocidades, formatos de tiempo y espacio electrónicos; transmiten (emitir/recepcionar), almacenan (en hard disk, discos flexibles o compactos, o en unidades de backup), editan (copiar, borrar, mover) información digitalizada, bien sea textual, gráfica, imágenes fijas o móviles o sonido; todos son mecanismos idóneos, rápidos, eficaces, confiables, seguros para transmitir información o datos, de forma que se aprovecha al máximo las tecnologías TIC y la informática, pero son vulnerables y surge el riesgo, por la acción humana cuando con ellos se transgrede, desconoce, limite o nulite el ejercicio de un derecho, libertad o interés legítimo; y, finalmente son dispositivos eminentemente de software que funcionan en tanto tengan un sistema o aparato de hardware idóneo, tal como el relacionado en los apartes anteriores de este trabajo. La diferencia de cada dispositivo se marca en el diverso uso dado a los mismos y las características especiales que daremos de cada uno.

A priori, comentaremos de los mensajes de correo electrónico (*E-Mail*), a los que las normas penales españolas hacen referencia expresa en el C.P.Esp., v.gr. Art. 197-1. En igual forma comentaremos, los foros de debate o grupos de discusión (*Newsgroups*); los servicios de lista de correo electrónico (*Mail Exploders o List Servs*); las conferencias en tiempo real (*Chat rooms*) y La red de redes de información a través de las páginas de hipertexto o hipermedia (*W*orld *W*ide *W*eb:WWW)

---

(104) *Abonado.* "La persona física o jurídica que sea parte en un contrato con el proveedor en un servicio público de telecomunicaciones para la prestación de tales servicios". (Art. 2-a, Ibídem).

(105) *Usuario.* "La persona que utiliza un servicio público de telecomunicaciones con fines privados o comerciales, aunque no haya contratado dicho servicio". (Art. 2-b, Ibídem).

4.3.3.1. LOS MENSAJES DE CORREO ELECTRÓNICO: EL "E-MAIL".

Cuando un usuario de ordenador deja de utilizarlo como un medio potente de almacenar, organizar y procesar información, para otros fines, como el de transmitir (emitir/recepcionar) información o datos de cualquier tipo con otros ordenadores conectados a través de una línea telefónica, un MODEM, una red de comunicación e información, decimos que el usuario ha ingresado en el fascinante mundo de la cultura electrónica, la lógica electrónica del *ON LINE*; en la visita virtual a diferentes lugares del planeta, a recorrer las "autopistas de la información" en la "aldea global" de *Marshall* **[106]**, y lo que es aún más espectacular, a recorrer el mundo de la información, la comunicación sin abandonar su casa **[107]**, su sitio de trabajo, su universidad, etc., pues para entrar y salir de un sitio virtual no existen fronteras geográficas, peajes y casi ni controles.

El correo electrónico es aquél que con idénticos fines y propósitos del correo tradicional, se envía y/o recibe mensajes con información o datos (textuales, imágenes o sonido) y se hace por medios, formatos (de espacio y tiempo v.gr. "textos enriquecidos" con formatos HTML -- de hipertexto o hipermedia--, es decir, formatos para páginas WEB), maneras de almacenamiento, edición, trasmisión y velocidades electrónicas. Sirve para la comunicación entre personas a través del mismo ordenador que se utiliza para el trabajo habitual con el consiguiente ahorro de tiempo y de papel o de llamada telefónica **[108]**.

El cuerpo del mensaje a enviar y/o recibir, tiene una estructura básica, sea cual fuere el software que se utilice para crearlo: a) Un encabezado del mensaje (*header*) con los datos del destinatario e información similar; y b) El mensaje propiamente dicho, denominado también "cuerpo del texto" (*body*) **[109]**.

En el *header* se colocan los datos del destinatario (Para:) que básicamente son:
a) la dirección electrónica, compuesta por un nombre alfanumérico (máximo de 11 caracteres, como regla) adoptado por la persona, el vínculo universal --"@"--, el servi-

---

(106) McLUHAN, Marshall. Citado por DEL PESO NAVARRO. LA SEGURIDAD. Ob. ut supra cit., p.1
(107) BENEDIKT, Michael. Citado por KATSH, Ethain. *RIGHTS, CAMERA*... Ob. Ut supra cit.
(108) DEL PESO NAVARRO, E., Ob. cit., pág. 213.
(109) TORBEN RUDOLPH, Mark. *TODO SOBRE EL INTERNET EXPLORER 4.* Ed. Marcombo, Barcelona,1998, p.128.

dor de las comunicaciones, la institución o entidad (si hace parte de alguna, bien sea *EDU*cativa --cualquier nivel: EDU--, Gubernamental --*GOV*--, Empresarial, financiera o *Co*mercial --*CO*--, mundialmente reconocidas) y el país v.gr. ES: España, CO: Colombia, CA: Canadá, AU: Australia, UK: Reino Unido, etc; b) la dirección electrónica y con carácter facultativo de los que podríamos llamar "Codestinatario" o tercero ("cc:") y/u otros determinados ("cco:"), a quienes se puede enviar un mismo contenido de mensaje y de conocimiento de direcciones electrónicas, salvo a los últimos a quienes se envía el mensaje pero no las direcciones electrónicas del mensaje principal; y , c) El resumen del asunto o del contenido del mensaje ("Subject" o asunto). Se utiliza para hacer un pequeño abstract del cuerpo del mensaje que identifique al destinatario de *prima visu*, quién, qué y por qué, se envía un mensaje. Esto ahorra tiempo y concreta el mayor o menor interés por la lectura mediata o inmediata del mensaje. Este "subject", es una especie de "Ref:" en la carta tradicionales, y quizá sea éste una reminiscencia de la lógica de la cultura de la escritura o del impreso.

El Remitente del mensaje se identifica ante el destinatario con su dirección electrónica (compuesto con un nombre alfanumérico y una ruta o camino electrónico con distinción universal. v.gr. LORG@udenar.edu.co. Significa: Nombre y apellidos del remitente, el servidor de la comunicación, la institución educativa universitaria--Univ.de Nariño-- y el país --Colombia--), que irá incorporada en el *header* del destinatario, o también con su firma electrónica en forma facultativa para imprimir mayor seguridad a sus mensajes, evitar falsificaciones, modificaciones que pueden producirse durante la ruta de envío. La firma electrónica puede consistir en la inserción de un gráfico, que bien puede ser la rúbrica habitual escaneada (o rastreada mediante *"scanner"* o periférico de ingreso de información I/), por ejemplo, en forma de "mapa de bits" que ocupa bastante espacio en memoria; o en forma digital, previamente creada por el remitente antes de enviar el mensaje electrónico para asegurar además, al destinatario la confiabilidad de quien envía dicho mensaje, que no se trata de un "remitente falsificado" (*fake* **[110]**) y que el futuro la firma digital será automáticamente insertada en todo mensaje enviado por el remitente, distinguiéndolo inequivocamente.

Esta firma electrónica, se diferencia de la identidad electrónica personal o dirección electrónica (*ID*:) antes vista y de la clave, contraseña electrónica o llave electrónica del buzón de correo ("Password"). En efecto, el ID, describe alfanumericamente y señala la ruta electrónica del usuario y la clave o llave electrónica, es el conjunto de caracteres numéricos o alfabéticos de carácter secreto creados por el

---

(110) Estos Fake´s, como mínimo juegan con bromas, "enviado mensajes electrónicos del Papa, del Presidente o de Elvis Presley..." . Ibídem, pág. 131.

usuario para acceder a su buzón electrónico, y por tanto, sólo está alcance y conocimiento del titular. Esta serie caracteres (que en el monitor del ordenador, pese a ser símbolo, número o letra, se esconden bajo tantos asterísticos "******* "como caracteres empleados por el usuario), constituyen una llave electrónica o clave de acceso al buzón personal de correo que difícilmente puede ser alterada por personas diferentes a su propietario, a no ser de que tenga conocimientos avanzados de manipulación de software o programas de ordenador que permitan conocer la estructura interna de esos caracteres, que por regla general, están en "lenguaje de máquina" incomprensibles a simple *visu* del ser humano. Si por alguna razón se olvida la clave el titular, el software de correo electrónico, puede asignarle otra clave automáticamente previa la interrogación y contestación correcta del usuario de una pregunta que sólo usuario y software conocen. Sin embargo, esta clave nueva, como la original podrá ser cambiada por voluntad del titular cuantas veces quiera desde dentro de su buzón electrónico. Es más, una regla de oro en la seguridad del correo electrónico, aconseja cambiar la clave continamente, eso sí, grabándosela únicamente en la memoria humana.

Cada usuario de correo electrónico posee desde el mismo momento en que adquiere el servicio de correo con un proveedor del software de comunicaciones, a través de un servidor institucional (educativo, gubernamental, laboral, etc), vía WWW (Word Wide Web) y previa la suscripción de un contrato de adhesión o aleatorio, con la empresa propietaria de los derechos de autor del software de correo electrónico. Contrato que sólo aparece con un simple epígrafe de "*I Accept*"**[111]**, pero que contiene una compleja estructuración y cláusulas que abordan temas técnicos (software y hardware); jurídicos (obligaciones, derechos y responsabilidades) ; y, sobre todo, de carácter preventivo en caso de utilizar negligente o dolosamente el correo electrónico, o de hacerlo para transmitir propaganda inútil ("junk mail"), correo basura ("Spam"), cartas en serie (" Chain letters"), o distribución masiva de correo electrónico no solicitado por un usuario (sumario de la cláusula c, del contrato "*I accept*"). Este carácter se endilga particularmente a proteger los derechos fundamentales de la persona como el de la intimidad (*Privacy*) y la propiedad intelectual (*The intellectual property*).

---

(111) El Contrato "***I accept***" suscrito electrónicamente por el usuario con la empresa servidora y propietaria de los derechos intelectuales del Software, YAHOO MAIL y FOUR11, que hemos tomado como ejemplo, contiene 2O cláusulas que hacen referencia a los siguientes temas: I) Acknowlegment and acceptance of terms of service; II) Description of service; III) User´s registration obligation; IV) Use of registration date; V) Modifications of terms of service; VI) Modifications of service; VII) Yahoo Mail Privacy Policy; VIII) Member accourt, password and security, IX) Member conduct; X) Indemnity; XI) No resole of service; XII) Email Storage; XIII) Termination; XIV) Dealings with advertisers; XV) Links; XVI) Yahoo proprietary rights; XVII) Disclaimer of warranties; XVIII) Limitation of liability; XIX) Notice; XX) General. Via internet. Texto completo en *inglés en:WWW.YAHOO.COM.*

A título de ejemplo citemos una de las cláusulas de un contrato "*I Accept*" , el cual se refiere a los tópicos anotados. En efecto, se sostiene:

> *Política de protección de la Intimidad. La Empresa de servicio de correo electrónico YAHOO considera E-mail al transmitido por esta vía y que tiene por objeto la correspondencia privada entre el remitente y destinatario. YAHOO, no supervisa, revisa o descubre los buzones de los usuarios de las comunicaciones privadas, salvo que el usuario lo consciente y YAHOO y su operador del servicio "Four11" pueden hacerlo, por las siguientes causas: a) Porque ha sido requerido por la ley; b) En cumplimiento de una orden o procedimiento legal; c) Si fuere necesario para dar fuerza a las reglas preventivas y de protección de los derechos (The "YMTS)"; d) Para responder a las demandas o reclamaciones por violación de derechos de terceras personas; e) Para proteger los derechos de propiedad intelectual de YAHOO y su operador "Four11", o de otros usuarios conocidos.*
>
> *Los usuarios están de acuerdo que el proceso técnico por el cual se lleva a cabo la comunicación del E-mail, puede ser requerido para: a) para enviar y reciba mensajes; b) para acceder a los requerimientos técnicos de las redes que conecten; c) para acceder al servicio conforme a las limitaciones de servicio ofrecido; o d) para hacerlo conforme a otros o similares requerimientos técnicos.*
>
> *El usuario reconoce y está de acuerdo con YAHOO y "Four11" (ordenador matriz) en no ceder ("endosar") los contenidos de cualquier comunicación . Sin embargo, estos no son responsables por cualquier acto ilegal, injurioso, difamatorio; o que invada la intimidad del titular o de otros; o, se trate de actos abusivos, dañosos, vulgares, obscenos o de tortuosos. Igualmente si se trata de actos objetivos que infrinjan la propiedad intelectual u otros derechos de la persona humana (Cláusula VII. YAHOO MAIL PRIVACY POLICY).*

Los buzones electrónicos, son los sitios electrónicos donde se almacenan los mensajes de correo, para diferentes fines: a) para que puedan ser organizados por orden de fecha de llegada, tamaño del mensaje, nombres de destinatarios, contenidos, etc., por períodos de tiempo definidos o indefinidos (aunque en informática esto sea un término inapropiado por la redefinición de tiempo y espacio), b) para ser leídos y contestados secuencialmente; c) para ahorrar espacio y tiempo; aunque, eventualmente se pueda acceder a la información mediante periféricos idóneos para corporeizarla en forma impresa. v.gr. con impresoras o plotters como

documentos printout; d) para transmitirla electrónicamente a terceras personas a quienes interesa o afecta el contenido del mensaje. Los programas de software que incluyen el servicio de correo electrónico disponen en el *header*, de un (cc: con copia), para cumplir con este cometido, e incluso con un (cco: con copia a otros), que a diferencia del destinatario principal (Para:) y el "codestinatario" (tercero), "no podrá ver a qué otras direcciones (electrónicas) se ha enviado el mensaje" **[112]** .

---

(112) Ibídem., págs. 194-195.

Los mensajes de correo electrónico, fueron pensados y diseñados para que, en principio, sólo remitente y destinatario conozcan el contenido a través de la simple escritura y lectura, respectivamente. Sin embargo, "en su camino del remitente al destinatario, los E-Mails circulan por una serie de ordenadores distintos y los administradores del sistema que así lo deseen pueden echar un vistazo al texto. Al fin y al cabo, el texto contenido en el paquete de mensajes que circula por la red puede leerlo cualquiera"**[113]**. Se asimila a los mensajes de correo electrónico "como una postal porque va destinada directamente al destinatario pero los trabajadores de correos pueden leerla durante el camino" **[114]**.

Más aún, pueden ser leídos por quienes no son sus titulares, cuando manipulan un mismo ordenador dos o más personas, ya sea un lugar de trabajo (oficinas, despachos, etc), en una aula informática educativa (de todos los niveles de educación tradicional o profesional), en un Centro, Institución o Entidad pública o privada, etc., donde el ordenador es un simple dispositivo o aparato de comunicación con otras terminales u ordenadores que pueden estar situados en cualquier lugar del planeta. En la mayoría de los casos, los software de comunicación por ordenador, vía internet, que poseen correo electrónico, permiten mantener en su memoria una serie de casilleros electrónicos, estilo "apartados de correo" para que cada usuario tenga su buzón particular. No en pocas veces, el buzón electrónicamente queda abierto por error del usuario, por daños en el uso del software, por daños en la red; en fin, por diversas causas. Al quedar abierto, uno cualquiera de los multiusuarios de un correo, puede optar por las siguientes alternativas: a) Una correcta, por acción y omisión. Por lo primero, procederá a cerrar el buzón sin leer ni hacer acción alguna para alterar, editar o borrar el correo electrónico que no le pertenece. Por lo segundo, no utilizará el ordenador o lo "apagará" ; b) Una incorrecta, consistente en leer el correo del que no es titular. Si su curiosidad lo lleva más allá, comenzará a manipular los mensajes de correo, alterando, editando o peor aún borrándolos total o parcialmente. Estas actividades las puede llevar a cabo el intruso por error, negligencia o intencionalmente; c) Una actividad que podrá lindar el Código Penal. No sólo leer en pantalla el mensaje de correo, sino copiar,

almacenar o transferir el contenido en la memoria central o auxiliar (discos) del ordenador para luego, manipularlo de manera dolosa en perjuicio del titular del correo, en las variadas formas que la conducta humana sugiera. Las actividades de los literales ***a,*** y ***b***, son in memoria, en el literal ***c***, son actividades *output* (por impresión, por comunica

---

(113) Ibídem., págs. 194-195.

(114) Ibídem., págs. 194-195.

ción o por copia) reconvertibles a *in* de memoria (puede ser un *input*) de otro ordenador u otros dispositivos de almacenamiento de información (discos, unidades de backup, etc.,), o incluso en el mismo ordenador.

Para evitar que el correo electrónico se convierta en una postal leída por quien pueda y quiera hacerlo, es preciso colocarles una especie de "sobre cerrado" a los mensajes, consistente en cifrarlos (o encriptarlos) y así, "tan sólo quien dispone de la autorización electrónica para descodificar el código correspondiente puede leer el contenido" **[115]**.

Con la codificación, el texto se transforma --mediante un proceso matemático-- en una secuencia que aparentemente carece de sentido. La red por la que se transporta la información es la misma que para los mensajes no codificados, pero los mensajes codificados sólo pueden ser leídos por quienes están autorizados para hacerlo, a través del "código individual". Así, es posible "esconder" el contenido del mensaje de los intrusos por negligencia o dolo (hackers o crackers), y más aún, validarlos. En efecto, el proceso de codificación "dispone de un mecanismo de comprobación digital con el que puede determinarse si un mensaje ha sido modificado de algún modo en la ruta del remitente al destinatario. Este mecanismo es un modo de ´firmar electrónicamente´ los mensajes" **[116]**. Existen actualmente productos de software que hacen "más seguros" los E-Mails, utilizando "claves" o "códigos electrónicos", cuando se navega por Internet **[117]**. Técnicamente cada día los mensajes de correo electrónico se emiten y recepcionan en una órbita de confidencialidad y seguridad amplios.

Finalmente, los mensajes de correo electrónico, una vez han cumplido su

---

(115) Ibídem., págs. 194-195.

(116) Ibídem., págs. 194-195.

(117) "Para que estos procesos funcionen, son necesarios las claves con las que, en el marco de un proceso matemático, los mensajes puedan codificarse por parte del emisor y descodificarse por parte del destinatario. Para ello, *Outlook Express* (software de Microsoft) emplea el proceso S/MINE. Esta abreviatura viene de la expresión ´*Secure Multipurpose Internet Mail Extensions*´

(Aplicaciones múltiples seguras para el correo de internet) y utiliza como claves lo que se conoce como ´certificados´ (llamados también ´IDs digitales´. ID: *Digital personal*. Otorgados por oficinas Independientes). De este modo cada usuario utiliza dos certificados: uno público y otro privado. El público puede concederse a los demás participantes y sirve para poder asegurar los mensajes dirigidos a usted. Este tipo de mensajes sólo puede desprotegerse con el certificado privado, que no debería darse a conocer". Existen otras tecnologías de claves como, por ejemplo, el programa *Pretty Good Privacy* (PGP). TORBEN RUDOLPH, Mark. *TODO SOBRE EL INTERNET*... Ob.cit., pág. 195.

objetivo y propósito general, es decir, llevar y traer información clara, precisa, oportuna y eficaz, entre destinatarios y remitentes, podrán ser guardados o editados por sus propietarios o titulares. En efecto, se podrán facultativamente "guardar" o gravar ("*save*") en la memoria principal del ordenador o las auxiliares (variopinta clase de discos electromagnéticos), o editarlos, a través del software adicional suministrado con el de transferencia (emisión/recepción) de mensajes electrónicos.

En la edición ("Edition") de los mensajes electrónicos se incluye el borrado ("erase") o eliminación ("Delete") de los mismos. Se llega a este procedimiento, únicode los documentos electrónicos, para liberar espacio en la memoria del ordenador, y por ende, espacio en el buzón electrónico de los usuarios del correo, brindándole un espacio fresco para los nuevos mensajes y los no leídos aún ("UnRead"). Adicionalmente, como una medida de protección y seguridad de los interesados, para que permanezca menos tiempo en la memoria del sistema de la red de información general (v.gr. Internet).

4.3.3.2. LOS FOROS DE DEBATE O GRUPOS DE DISCUSION (THE NEWSGROUPS). LOS *E-MAILS POST*.

Los *Newsgroups* han sido catalogados como uno de los métodos de comunicación y de obtención de información, a través del acceso a la Internet. Por este método se puede transmitir textos, pero además, podría transmitirse sonido, fotos e imágenes en movimiento. Esta herramienta constituye un medio de comunicación unitario y único, lo que se ha venido en llamar *ciberespacio*, que aunque no se encuentra ubicado en ningún lugar geográfico, está abierto a cualquiera que tenga acceso a Internet, desde todos los puntos cardinales **[118]**.

Podríamos definir a los *newsgroups*, como aquellos grupos de personas que interconectadas por medios informáticos, electrónicos o telemáticos (lo que se significa tener un hardware y software idóneos para la comunicación electrónica **[119]**) desde cualquier lugar del planeta , intercambian informaciones o datos que pueden constituir lo que se conoce como "noticias", sobre algo o alguien. Las une el interés sobre la

(118) Sentencia del Tribunal Supremo de los EE.UU., de 26 de Junio de 1997. En: WWW. UNI-MUENSTER. DE/JURA/NETLAW. Citado por BARNEZ VASQUEZ, Javier. *LA INTERNET Y EL DERECHO, UNA NOTA ACERCA DE LA LIBERTAD DE EXPRESION E INFORMACION EN EL ESPACIO CIBERNETICO.* En: Revista C.G.P.J., Ordenación de las telecomunicaciones. Núm. VI, Madrid, 1997, pág. 239.

(119) Veáse, 2.41. y 2.4.2. Parte III.

temática informada, la capacidad de análisis y el provecho que de ello pueden obtener. Las temáticas que *facto* se van formando, van concentrando un inicial caos de información para conformar una especie de páginas electrónicas que al igual que las en un periódico o revista tradicional, conforman secciones, subsecciones de un mismo paquete de información o de noticias, que bien podría dividirse en asuntos políticos, deportivos, de opinión, económico-financieros, culturales, lúdicos y de ocio, etc. Si también se hace a la idea de que no existe redacción ni fecha de entrega para esa especie de periódico, sino que todos los participantes están sentados frente al ordenador en sus respectivos puestos y leen y escriben las noticias electrónicas a través de Internet cuando les place, se habrá formado una idea bastante aproximada de los que significan los Grupos de noticias **[120]**.

Los *newsgroups* y los llamados *E-mails*, técnica como jurídicamente tienen similares formatos, características y funciones, pero también tienen diferencias. En efecto, los *newsgroups*, manejan un lenguaje propio cada vez más complejo dentro de la lógica electrónica, a fin de ir diferenciándola de la lógica tradicional. Así, un mensaje electrónico enviado por un usuario a uno de estos grupos, se denomina *artículo* y el proceso de publicación se denomina *Post* **[121]**. A su vez, hay que diferenciar los mensajes electrónicos enviados entre usuarios (remitente/destinatario) con carácter particular o también conocidos como *Emails* y los mensajes también electrónicos enviados por un remitente a los *newsgroups*, pues aunque nacen con formatos, contenidos y velocidades electrónicas similares a los *e-mails*, la recepción y posterior publicación ("*post*"), los convierten en mensajes electrónicos públicos o de dominio popular. Podrían llamarse *e-mails post*, a los mensajes que surgiendo como mensajes particulares, por el efecto de la publicación y dominio público al llegar a los grupos de noticias, dejan de ser una privados para convertirse en públicos.

Sin embargo, tanto *e-mails* como los *e-mails post*, contienen similares formato de construcción electrónica. Esto es, contienen un *header* y un *body* **[122]** similar con algunas variantes en la composición. Los e-mails post, tienen: 1. Un *header* o encabezado con los siguientes items: a) Nominación del "Grupo de Noticias", al cual va dirigido el mensaje electrónico, que por regla general será una especie de destinatario

_____

(120) TORBEN RUDOLPH, Mark. *TODO SOBRE*... Ob. ut supra cit., pág. 144.
(121) Ibídem, pág. 153.
(122) Ibídem, pág. 155.

grupal caracterizado según el temario, tal como veremos más adelante ; b) El "subject" o un mini-resumen del asunto a tratar. Es el "Ref:", de la lógica escrituraria; c) La dirección electrónica de un codestinatario o "cc:", que significa: "*carbon copy*" (papel copia). Aquél codestinatario (individual o grupal), conocerá el tema y la ruta electrónica del mensaje; y, 2. El *body* o cuerpo del mensaje electrónico. Por regla general, de carácter textual, aunque no se descarta sonidos e imágenes fijas o móviles. Al final del texto irá el nombre y apellidos o seudónimo del remitente del mensaje electrónico. La dirección electrónica o "ID´s" del remitente se insertará automáticamente en el mensaje al ser recepcionado por el destinatario o destinatarios. El password utilizado por el remitente como clave o llave alfanumérica secreta, igualmente puede ser utilizado en e-mails como e-mails post, con idéntica función y *sigilium* de acceso electrónicos.

Los *newsgroups*, entonces, son inicialmente mensajes electrónicos individuales y determinados que cualquier persona del mundo puede enviar y recibir permanente e intemporalmente sobre la temática que se quiera, aunque luego se agrupan temáticamente. Estos mensajes electrónicos desde el momento que se "cuelgan" en esas páginas WEB de Internet, se vuelven de dominio público, y por ende, la responsabilidad social y jurídica de lo informado o recepcionado se extiende a la derivada de la libertad de expresión e información, con la limitaciones que establece el ordenamiento jurídico vigente de los Estados y el derecho de los demás, los derechos fundamentales que aquéllas conciernen (incluida la intimidad) . *De facto*, inicialmente y luego por la temática tratada en cada sección o subsección de esas páginas electrónicas o WEB, se conforman *los grupos de noticias* que tienen como autores determinados o determinables a un conjunto de personas identificadas plenamente con sus datos personales (nombre, apellidos, direcciones, profesión, etc.); o bien, identificables electrónicamente (mediante los ID´s o identidad digital que indica un nombre alfanumérico y una dirección electrónica), o mediante seudónimos alfanuméricos con ruta electrónica que permiten el anonimato.

Una vez conformados los grupos temáticos de noticias, sus autores o integrantes pueden conformar especies de "mesas redondas", para no sólo intercambiar las noticias sino analizar, debatir y contrastarlas con quienes tengan interés de hacerlo. Lo que inicialmente es aparentemente un caos de datos, puede organizarse de tal forma que la temática impone reglamentos consuetudinarios, decantados en la lógica tradicional o escrita y trasladados a la lógica electrónica por asimilación. Así , puede existir una especie de moderador o moderadores

según la temática y tantos participantes como informadores o usuarios del *newsgroups*. Esta interactividad en el intercambio de información o datos de todo tipo es lo que cataloga a los inicialmente *newsgroups* como foros de debate o grupos de discusión temática. La interactividad puede ser activa o pasiva, según la intervención del participante. Unos y otros participan y disfrutan de la lectura en el monitor de las noticias en tanto estén interconectados (*On line*, o incluso *Off linea*, según la capacidad del software servidor de éste método de comunicación entre ordenadores, con lo cual se ahorra tiempo y dinero, máxime si el usuario esta conectado a la red mediante una línea telefónica particular [123]).

Los diversos software que permiten el servicio de *newsgroups* en sus ordenadores, permiten entre otras funciones, las siguientes: a) La suscripción personal a los grupos de noticias existentes en el mundo, según la capacidad, calidad y la temática ofrecidas por el servidor y requeridas por el usuario; b) La modificación posterior a la lista de grupos de noticias a la que se ha suscrito el usuario; c) Una guía preliminar sobre los actuales grupos de noticias existentes y su significancia. v.gr. ***es*** Todos los grupos que empiezan con la abreviatura *"es"* son en español; ***misc***. La abreviatura *"misc"*, es miscallenous (miscelánea); ***mag.*** Revistas de todo tipo, publicaciones periódicas; ***org.*** Diversas organizaciones. p.e.: clubes de informática, también empresas o universidades; ***rec.*** Recretational Activies o actividades recreativas. Es decir, el tiempo libre, desde fútbol, pasando por juegos, hasta literatura; ***sci.*** Science (sci). Temas científicos; ***soc***. Social. Temas sociales; ***etc.*** etcétera. Se agrupan todos los temas que no pueden clasificarse en otro lugar, ***alt.*** Aquí encontrará una jerarquía "alternativa": puesto que existe un procedimiento muy complejo para introducir nuevos grupos en la jerarquía existente (funciona mediante propuestas, discusiones y votaciones), se ha establecido una segunda jerarquía paralela en la que se ha facilitado enormemente la incorporación de nuevos grupos. Por el momento funciona de forma bastante caótica, de modo que nadie tiene realmente una visión global de todos los grupos *alt* incorporados; y , ***D.*** Algunos grupos moderados, es decir, que los artículos que se envían allí no se mandan inmediatamente a todo el mundo, sino que el moderador del grupo primero comprueba su relevancia y, dado el caso, los separa (p.e., porque los mensajes deben limitarse a anuncios importantes de una organización). En tales casos, con frecuencia existe para ese foro de debate otro grupo con una letra *d.* detrás del nombre. Se trata entonces de un foro adicional establecido especialmente para debatir libremente sobre el tema en cuestión; d) Una guía de listas de servidores de noticias

---

(123) Ibídem., pág. 155

públicas, sobre diversa temática y dentro de los anteriores grupos de noticias [124]; y, e) Una libreta de direcciones con todas las direcciones de correo electrónicos junto con el nombre, las señas personales y profesionales, con la posibilidad de llamada a través de *NetMeeting* seguridad mediante ID digital [125]. Esta libreta puede ser editada y organizada conforme a las posibilidades del software y las necesidades del usuario. La libreta facilita el envío de mensajes a rutas electrónicas conocidas, según los temas abordados y con máxima seguridad y ahorro de tiempo e incluso permite enviar mensajes tipo "circulares" a una serie de destinatarios que sería lento y engorroso hacerlo por medio del "cc:" del *header* del mensaje electrónico.

De otro lado, tanto los *e-mails*, como los *e-mails post*, enviados a los newsgroups, son medios de comunicación electrónica que no han sido diseñados, según *Jarvlepp* [126], como instrumentos eficaces de protección y seguridad de la intimidad de las personas (" the privacy") cuando se navega por Internet, puesto que en las rutas electrónicas de envío/recepción de mensajes electrónicos éstos pueden interceptarse fácilmente o pueden copiarse sin dejar cualquier rastro e incluso puede modificarse ruta o dirección electrónica del mensaje. Igualmente, porque en nuestro criterio, desde el momento mismo que se envía un mensaje electrónico a un destinatario individual (e-mail), o más aún a un destinatario grupal (e-mails post en los newsgroups), el autor o remitente es consciente de que parte de su banco secreto de datos o informaciones personales, secretas o íntimas es abierto para que puedan ingresar en él legítima o ilegítimamente (por error, negligencia o dolo), pues ha hecho una especie de depósito o ingreso de parte de esa intimidad al gran banco de datos que circula por las redes de información del mundo (v.gr. Internet), donde cual más cual menos, puede acceder a ese banco público de datos para ojear u olisquear datos o informaciones que no le pertenecen o que por error o negligencia de un servidor de comunicaciones le llega equivocadamente a su destino, o en fin, que los mensajes se pierden de su ruta electrónica. Un usuario de medios electrónicos cada día cede voluntariamente parte de su intimidad desde el momento mismo que hace uso de uno cualquiera de ellos.

---

(124) Ibídem, págs. 147-148.

(125) Ibídem, pág. 159-160

(126) JARVLEPP, Harry. B.A., LL.B, M.B.A. Lawyer Information Technology Law. AN INTRODUCTION TO THE LAW OF THE INTERNET. PI. En: Revista "*KNOWLEGDEBASE. AN INFORMATION TECHONOLOGY LAW BULLETIN-SPRING. 1995*." Texto completo en WWW.UMONTREAL. EDU.CA.

4.3.3.3. LOS TABLONES ELECTRONICOS DE ANUNCIOS O *"ELECTRONIC BULLETIN BOARD SYSTEM "*: ALMACENAMIENTO, ACCESO E INTERCEPTACION DE INFORMACION.

Si bien el estudio pormenorizado de los sistemas electrónicos de anuncios comerciales o financieros, a través de tablones que navegan por las red de redes de la Internet o de cualquiera otra que tenga cobertura, características y funciones en la sociedad informatizada, pertenece más al derecho privado y mercantil, aquí hacemos referencia a este medio electrónico de comunicación, a los efectos de ser uno los instrumentos más idóneos de almacenar, organizar, transferir y consultar mensajes de correo electrónico (E-mails), con fines mercantiles y comerciales sí, pero que pueden llevar aparejada la transgresión o vulneración de derechos fundamentales, y en especial el derecho a la intimidad. Y, es precisamente sobre este último particular lo que aquí nos interesa destacar.

En efecto, los sistemas electrónicos de tablones de anuncios, para ser reconocidos como tales deben contener una estructura técnica (software y hardware) y jurídica propias de la empresa mercantil o financiera privada y/o pública, según el caso, que tienen como objetivos principales; entre otros, la negociación de bienes o servicios mercantiles, a través de la publicitación electrónica en las páginas WEB de la Internet o cualquier otra red de comunicación electrónica, a un número de personas o usuarios ("clientes electrónicos"), previamente admitidos y determinados mediante la cumplimentación de un formulario electrónico y clasificados según sus necesidades de negociación de bienes o servicios. Desde el punto de vista técnico los *Electronic Bulletin Board System*, son posibles si cuentan con un software y hardware idóneos para el ingreso, almacenamiento, organización, transferencia y consulta de mensajes de correo electrónico. Desde el punto de vista jurídico, el establecimiento o entidad comercial o financiera privada o pública debe haberse constituido como tal, según el ordenamiento jurídico vigente de cada Estado.

Los clientes electrónicos desde el momento en que han sido admitidos en el *Electronic Bulletin Board System*, manejan una dirección, identificación y password electrónicos propios, a efectos de reconocimiento, determinación y personalización de la necesidad de bienes y servicios. Los usuarios se comunican con los tablones electrónicos de anuncios mediante los mensajes de correo electrónico y son almacenados y procesados mediante sistemas informáticos, electrónicos y telemáticos por éstos. Por ello, tenemos que fundamentalmente este sistema electrónico se lleva a cabo mediente la emisión/recepción de mensajes de correo electrónico, el procesamiento por medios idénticos de una establecimiento comercial y financiera que anuncia sus productos en las páginas WEB, y actúa como una especie de almacén electrónico de los mismos (con software o hardware: hard disk, backups, discos flexibles o compactos, etc), los organiza, clasifica y emite

órdenes de cumplimiento a los departamentos, secciones o personas que deben cumplir con las solicitudes o demanda de bienes o servicios de los clientes electrónicos, confirmándoles por esta misma vía su cumplimiento.

En un reciente caso norteamericano [127] que tuvo por fundamento la incautación de medios informáticos de software y hardware, por parte de los Servicios Secretos de los Estados Unidos (United States Secret Service and United States of América), por presunta comisión de actos ilícitos de una de las personas colaborador del operador del sistema electrónico de tablón de anuncios (*"Electronic Bulletin board system")*, denominado *"Illuminati. BBS*", el cual manejaba información sobre negociación de libros, revistas, folletos, y publicaciones, en general.

En las memorias centrales y periféricas del computador que almacena y procesa información por medios informáticos, electrónicos o telemáticos, fueron los objetos materiales e intangibles de la incautación por parte del *Secret Service US*. Según los demandantes en primera instancia, luego apelantes; entre ellos, Steve Jackson Games (SJG) *et all*, el sistema electrónico del BBS, contenía varios mensajes privados de correo electrónico enviados por potenciales clientes o personas interesadas en el ofrecimiento comercial operador del " BBS. Illuminati". Los mensajes se almacenaban en la memoria del *hard disk* del ordenador y también en una copia de seguridad o *backup*. Los mensajes así almacenados, no alcanzaron a ser leídos por la empresa destinataria, cuando fueron incautadas por el *Secret Service US* . Los destinatarios una vez leídos los mensajes electrónicos, pudieron haber optado por guardarlos en memoria

---

(127) Cfr. STEVE JACKSON GAMES, INCORPORATED, et al., Plaintiffs-Appellants, v. UNITED STATES SECRET SERVICE, et al., Defendants, United States Secret Service and United States of America, Defendants, Appellees. No. 93-8661. United States Court of Appeals, Fifth Circuit. Oct. 31, 1994. Peter D. Kennedy, R. James George, Jr., George, Donaldson & Ford, Austin, TX, for appellants. Sharon Steele, Washington, DC, for amicus curiae Electronic Frontier Foundation. Scott McIntosh, Barbara Herwig, U.S. Dept. of Justice, Washington, DC, for appellees. Appeal from the United States District Court for the Western District of Texas. Before HIGGINBOTHAM, JONES and BARKSDALE, Circuit Judges. RHESA HAWKINS BARKSDALE, Circuit Judge: Abstract: " The narrow issue before us is whether the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read (retrieved) by the intended recipients, constitutes an unlawful intercept under the Federal Wiretap Act, 18 U.S.C. s 2510, et seq., as amended by Title I of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, Title I, 100 Stat. 1848 (1986). We hold that it is not, and therefore AFFIRM." Texto completo en: *WWW.UMONTREAL.EDU.CA.(Universidad de Montreal Canadá).*

central o auxiliar (*save*), borrarlos o anularlos (*delete*), una vez haya cumplido su finalidad, lo cual no pudo ser posible en el caso *sub lite*, porque se interceptaron antes de realizar una cualquiera de estas facultades del BBS. Según el Operador del BBS, en febrero de 1990, existían 365 usuarios y en Marzo 1, 162 usuarios [128] .

Steve Jackson Games et all, sostenía que el actuar de la Agencia Especial de EE.UU, constituía una intervención o interceptación ilegal de las comunicaciones electrónicas, en virtud de la Ley Federal de Comunicaciones por Cable. 18 U.S.C., enmendada por la Ley de Protección a la intimidad en las comunicaciones electrónicas de 1986 (*The Electronic Communication Privacy Act of 1986*). La Sentencia de la Corte de Apelaciones de los Estados Unidos de América, 5□ Circuito, Octubre 31 de 1994, estimó en el presente caso que no existió interceptación de las comunicaciones electrónicas, almacenada en disco y/o backup, aún no leídas por su destinatario, pues no se dieron los requisitos de fondo y forma para la mentada interceptación.

En efecto, entre otras razones técnico-jurídicas de la Corte Norteamericana para desatender las pretensiones de los demandantes estaba en que la interceptación ("interceptation"), al ser definida como la "adquisición auditiva o similar de cierto volumen o contenido de información o comunicación por cable ("Wire Communication"), electrónica ("Electronic Communication"), o en forma oral, a través del uso de cualquier dispositivo electrónico, mecánico u otros", según el artículo 2510 del *Act Wiretap*, 18 U.S.C., requiere de un elemento temporal fundamental para que la interceptación o intervención se cumpla, pues de lo contrario, ésta se desvirtúa, o lo que es lo mismo, no existe. En efecto, se sostiene que la "adquisición (debe ser) contemporánea a la comunicación (es decir, a la trasmisión: emisión y recepción del mensaje, sea cual fuere el medio: tradicional o electrónico), a través del uso del dispositivo" idóneo (software y/o hardware) [129].

La Comunicación electrónica, consiste en la "transferencia de señales, signos, escritura, imágenes, sonido, datos o informaciones de cualquier naturaleza transmitidas en todo o en parte por cable, radio o en forma electromagnética, foto-eléctrica o por

---

(128) Corte de Apelaciones de los Estados Unidos de América, 5□ Circuito, Octubre 31 de 1994, Caso Steve Jackson v. Secret Service US. En: *WWW.UMONTREAL.EDU.CA.*

(129) Fundamento Jurídico (FJ), No. 4 C.F.US, Oct. 31/94. En: *WWW. UMONTREAL.EDU.CA*. Los paréntesis son nuestros.

sistema foto-óptica y afectan al comercio entre estados o con el extranjero" [130].

El problema central que se debatió ante la Corte de Distrito Norteamericano (The District Court), en primera instancia era sin embargo determinar si se había o no vulnerado *La Wire Act Federal*, sí mediante las labores electrónicas del BBS, al recepcionar y enviar contestación a los mensajes de correo electrónico particulares, los cuales eran temporalmente

almacenados en la memoria del *hard disk* del ordenador de la *Electronic Bulletin Board System (BBS)*, hasta cuando fueran leídos por la empresa destinataria de la información. La *Wire Act Federal*, enmendada por *Electronic Communication Privacy Act* (ECPA), enmendada en su Título I, 18 U. S.C., artículos 2510-2521, proscribe *inter alios* la interceptación intencional de comunicaciones electrónicas; así mismo el Título II, artículos 2701-2711, que proscribe, *inter alios,* el acceso intencional, sin autorización a la comunicaciones electrónicas e información almacenadas. La Corte de Distrito sostuvo que el Secret Service Us, violó la ECPA y le confirió a los demandantes a titulo de indemnización por daños y perjuicios reales US$ 51,040 a SJG; así mismo que se violó el Título II de la ECPA, al interceptar las comunicaciones electrónicas almacenadas en memoria sin tener autorización ni obedecer las provisiones normativas que la prohíben. Sin embargo, entre otras declaraciones de la Corte, sostuvo que el Secret Service US, no interceptó los E-Mail particulares, según el Tit. I., de la ECPA, 18 U.S.C., artículos 2511 (1), a), porque " *la adquisición de los contenidos particulares de las comunicaciones electrónicas no eran contemporáneas con la transmisión de esas comunicaciones*" **[131]**. La Corte de Apelaciones norteamericana, se detuvo especialmente en el análisis de esta última parte, para confirmar ("Affirm") la Sentencia de primera instancia. No obstante, analizó un aspecto igualmente importante y sobre el cual hizo un énfasis añadido en el caso *sub examine*: el almacenamiento electrónico ("electronic storage") en la memoria central o auxiliar de un computador, pues según la dialéctica de la Sentencia este aspecto tanto en primera instancia como en la Corte de apelaciones, no fue previsto por el legislador en la ECPA, 18 U.S.C, artículo 2510, cuando usa el término "transferir" en las "comunicaciones electrónicas" y hace omisión en la definición de estas de la frase: *y cualquier almacenamiento electrónico en las comunicaciones* ("any electronic storage of such communication"). Esto refleja que el Congreso no pensó en la interceptación de las

---

(130) Punto 5.2.2.2. Al comentar la parte in fine del tipo penal atentatorio de la intimidad a través de medios informáticos, electrónicos o telemáticos, y más concretamente sobre la interceptación o intervención de las comunicaciones, haremos un pormenorizado comentario a las comunicaciones electrónicas diferenciadas de las comunicaciones tradicionales o por cable.
(131) Fundamento Jurídico (FJ), No. 4 C.F.US, Oct. 31/94. En: *WWW. UMONTREAL.EDU.CA*

comunicaciones electrónicas cuando estas están almacenadas **[132]**. Desentrañando el espíritu del ordenamiento vigente sobre comuni- caciones electrónicas y las enmiendas a la ECPA, la Corte concluye que al proscribir el Tit. II de la ECPA, cualquier acceso intencional sin autorización alguna a la comunicaciones alámbricas o electrónicas (art. 2710, a), el tema mencionado quedaría incluido, pero a la vez hay que distinguir lo que se entiende por acceso e interceptación de las comunicaciones electrónicas, pues el Secret Service US, se encontró que sin autorización legal o judicial, accedió a la información del BBS, pero no que las interceptó, como antes hemos analizado.

4.3.3.4. LAS CONFERENCIAS EN TIEMPO REAL ("CHAT ROOMS").

Este medio de comunicación electrónica se caracteriza porque constituye la trasmisión: emisión/recepción de mensajes electrónicos *on line*, en tiempo real desde cualquier punto del planeta entre personas que desean conversar electrónicamente sobre un tema predeterminado o que surge en el transcurso de la trasmisión, tal y como si se hiciera entre un grupo de personas parlantes en un salón, un café, un restaurante, una aula, etc. Para ello deben disponer de un software y hardware apropiados, estar conectados a un red de redes (v.gr. Internet), estar preparado para recepcionar y emitir mensajes en línea, sin retraso alguno o como se suele decir en el lenguaje televisivo, conversar electrónicamente (textual o mediante sonido digitalizado) en "directo". Los participantes pueden ingresar, intervenir y salir de una tertulia electrónica virtual del mismo modo que lo hicieran de una conversación física o real aunque con un lenguaje informático especial para la primera como no se acostumbra en esta última. Este es apenas obvio, pues los conceptos como el comportamiento ante estos nuevos medios de comunicación entre las personas, como se ha repetido varias veces, ha generado una lógica y cultura nuevas, que algunos como el profesor *Ethain* ha dado en llamar la "*cultura electrónica*".

Los Chat rooms son un servicio de comunicación electrónica en línea y en directo que patrocinan, ofrecen o incluyen como servicio añadido los medios de comunicación electrónica que circulan por la red de redes de información (periódicos, revistas, boletines, etc); así como también, los propietarios, distribuidores o concesionarios de software especializado en comunicaciones electrónicas (verbi gratia

---

(132) Fundamento Jurídico (FJ) No. 7 C.F.US, Oct. 31/94. En: *WWW. UMONTREAL.EDU.CA*

"Microsoft Chat" **[133]**). Igualmente, las innumerables empresas, entidades o centros públicos o privados e Instituciones de educación, especialmente a nivel universitario.

Todos ellos tienen un objetivo principal: vincular a sus usuarios a las temáticas que cada organismo ofrece según su ideología o filosofía propias, los puntos de convergencia que estos manejan o los aspectos tratados o por comentar, etc. Para el usuario, significa un instrumento idóneo de conversación electrónica sobre algún tema posibilitado por el aquéllos organismos, previa la identificación (real, por seudónimo o mediante un sobrenombre **[134]**) y la

determinación de una dirección electrónica, la correspondiente asignación de un *password* o clave electrónica y la prestación del servicio de comunicación *chat rooms* por un servidor en red.

Las *Chat rooms*, se diferencian de otros medios de comunicación electrónica, tales como: a) con los *NetMeeting*, que tienen por objeto las conversaciones electrónicas o "debates cerrados con participantes conocidos", pues los chat rooms, permiten estas charlas públicas en cualquier parte de Internet [135]; y , b) con los *newsgroups*, aunque se realiza con la metodología, fines y hasta objetivos de los chat rooms, aquéllos se desarrollan entre usuarios o personas y entre las cuales su conversación electrónica "no es en tiempo real", [136]como sí lo son los chat rooms.

---

(133) El Microsoft Chat es una especie de Chat rooms estructurado de dos formas: a) en modo de sólo texto (only text), que debe preferirse si se quiere aumentar seriedad a la tertulia o conversación; y b) en forma de tiras o figuras cómicas, al estilo de un periódico, revista o folleto. Este último esta desarrollado con metodología de un "comic" interactivo en el cual los participantes pueden escoger limitadamente de entre un número de personajes previamente determinados y caracterizados por el proveedor del software para que tengan conversaciones o charlas interactivas sobre un tema igualmente determinado y por el espacio de tiempo que escoja el grupo. Este ambiente de comic del Microsoft chat tiene ventajas y desventajas. Entre las primeras la facilidad con la cual los participantes ingresan a un grupo de charlas en directo y en línea, pues el objetivo principal de comic es divertir, relajar, enseñar y utilizar mejor el tiempo. Sin embargo, esa misma ventaja se convierte en una desventaja, pues la metodología utilizada por el proveedor esta bien para niños y adolescentes, pero no para todos los adultos. En efecto, los adultos que desean tener un chat rooms serio poco o nada tiene que ver la pedagogía del comic para ingresar, sostener, desarrollar y concluir una conversación electrónica. En el texto citado, se presenta ampliamente la metodología y desarrollo de este ambiente especial de chat rooms utilizado por Micrsosoft Chat. Véase. TORBEN RUDOLPH, Mark. *TODO SOBRE*... Ob. ut supra cit., pág. 225

(134) "El sobrenombre (es una especie de *alias*, o nombre único que identifica a un usuario o persona que utiliza este medio de comunicación) es el nombre que el resto de participantes del Chat podrán utilizar para hablar con usted. Por lo tanto, debe ir con cuidado al elegir su sobrenombre y debe hacer de forma que, si es posible, evite de antemano posibles conflictos con otros usuarios. Además, debe tener presente que todo lo que diga y haga en el chat se muestra bajo su sobrenombre. Una elección de nombre desafortunada podría provocar confusiones y, normalmente, no se toma en serio a las personas que eligen un nombre tonto o vulgar". Paréntesis nuestros. Ibídem., pág. 226-227

(135) Ibídem, pág. 225

(136) Ibídem, pág. 225

Los *chat rooms*, cada día se imponen como medios de comunicación electrónica entre un número de personas que sin salir de su casa, universidad, institución, centro u organismo privado o público, puede obtener una charla o conversación al estilo de las viejas tertulias de café o salones especiales. Constituyen una especia *sui géneris* de salones virtuales tan inmensos como puntos cardinales donde están ubicados los miembros o usuarios reales de esa extraña mesa planetaria que sin estar físicamente uno frente de otro, participan en tiempo real ("real time") y en directo en una tertulia predeterminada. Es especial esta constitución pues mientras la construcción de la mesa de conversación es virtual, la conversación o comunicación electrónica es real y en directo.

Hoy en día, existen tantos salones de charla, como servidores de comunicaciones electrónicas hay. Algunos software expertos en chat rooms, adminis- tran "una lista de salones

favoritos" [137], para evitar que sus usuarios naveguen sin brújula ni control en un mar de posibilidades de conversación, en esas nuevas zonas selváticas que genera el espectro electrónico, en las variopintas temáticas que seguramente no les interesa, o que sea mejor, prefieran no conocerlas. Igualmente, para evitar distracciones con exagerados dibujitos, gráficos u otros distractores que le resten profundidad, seriedad y reflexibilidad a las conversaciones electrónicas, los programas de ordenador especializados ofrecen los *chat rooms* en *Internet Relay Chat* (IRC)[138] o sistema de charla basado en el texto, que como se dijo antes debe preferirse a cualquiera otro, como este estilo de comunicaciones electrónicas.

4.3.3.5. EL HIPERTEXTO (HTML: HyperText Markup Language): PAGINAS WWW: WORLD WIDE WEB.

El Hipertexto es el hijo primogénito y más genuino de la información y comunicación electrónica. Con el nacimiento del Hipertexto no sólo se han establecido nuevas formas tecnológicas TIC en unión con la informática, sino una estructura de comunicación electrónica *sui géneris:* interactiva, global, sin límites geográficos y de trasmisión (emisión/recepción) de información de todo tipo, por universidades, instituciones, Centros u Organismos privados y públicos en formatos, con funciones, características y velocidades electrónicas, siempre y cuando se cuente con un software y hardware idóneos.

El Hipertexto, como otros medios de comunicación electrónica, está basado en

---

(137) Ibídem, pág. 243.
(138) Ibídem, pág. 243.

los términos anglosajones apocopados de *Hyper Text Markup Language* (HTML)[139], que gramaticalmente significa: Lenguaje textual gradualmente incrementado, aunque se ha difundido universalmente como hipertexto que subsume las características de gradualidad, vinculación e incremento, entendibles en nuestra lengua castellana con el prefijo "*hiper*". Igualmente se ha considerado el HTML, como el formato utilizado por las páginas de texto creadas exclusivamente para ser colocadas en una red de redes de información por el proveedor respectivo.

El Hipertexto tiene una forma (interna y externa) y un fondo.

La forma externa del hipertexto hace relación a la construcción textual con formatos de página WEB, es decir, con metodología World Wide Web (WWW); en tanto que la forma interna hace referencia a la parte técnica y configuración del sotfware apto para elaborar dichas páginas. Aquí, por obvias razones, nos referiremos a la forma externa, pues la interna es objeto de la informática estructural.

En efecto, para que un ordenador muestre toda la información en pantalla, y luego un usuario pueda emplearla informáticamente como cualquier información digital: almacenar (storage), editar (edit), transferir o simplemente consultarla en el monitor del ordenador debe crearse por parte de los proveedores de información (universidades, centros, etc), las denominadas páginas WEB dentro de un espacio de un servidor de internet denominado "*Webspace*" [140]. La publicación de páginas en el mundo virtual del WWW, conocida como *Webpublishing* [141] , siguiendo los pasos que determinan los diferentes software expertos, son: a) Disponer de un espacio nece sario en internet (Webspace), previamente determinado por un proveedor de servicios de comunicación electrónica; b) Con el software idóneo se crea las páginas WEB de información según las pautas, principios, características y funciones del proveedor de la información respectiva. Las páginas se escriben como si fuese con cualquier programa de ordenador que procesa texto común y corriente, pero con algunas diferencias técnico-estructurales, que no son del caso comentarlas ahora. Las páginas creadas y diseñadas de conformidad con los fines y objetivos del informador, se almacenan en memoria central y auxiliar del ordenador; y c) Las páginas creadas y almacenadas conforman lo que se denomina el *homepage* [142], o sea, las páginas matrices de la información que ofrece el proveedor

---

(139) Vid. El HTML. "Se trata de un lenguaje de descripción de páginas que reproduce el contenido y aspecto de la página WWW de tal forma que los diferentes programas de acceso (como Internet Explorer) pueden representarla con la forma que desee". TORBEN RUDOLPH, Mark. *TODO SOBRE*... Ob. ut supra cit., pág. 245

(140), (141) Ibídem, pág. 245.

(142) Ibídem, pág. 245

correspondiente. El proveedor de la información la enviará luego mediante su servidor de comunicación electrónica a la red de red de información (v.gr. Internet), para que comience a navegar en las autopistas de la información y sean utilizadas por los usuarios o internautas previo el acceso a la dirección y sitio de la red prefijado por el proveedor de la información.

Otras formas externa del hipertexto, lo constituyen las posibilidades que tienen las páginas WEB, para incorporar imágenes fijas y en movimiento (vídeo), ilustraciones o gráficos (dibujos multifacéticos) e incluso sonidos (voz, música o cualquiera otra fuente que genere sonido). Esta forma que constituye a la vez una de las principales características de las páginas WEB, conforman un ambiente especial de comunicación electrónica que une las ventajas y características de la multimedia [143] y las del hipertexto. Algunos iusinformáticos han llamado a este *sui* géneris y especial matrimonio tecnológico TIC y la informática como *Hipermultimedia* o simplemente *Hipermedia, según Marshall Brain* [144]. Quizá la principal virtud del hipertexto sea la alta capacidad para incorporar en sus páginas información textual, visual y de sonido, pues como nunca antes la información se presenta ante el usuario tranquila tranquilamente sentado frente a su ordenador situado en una aula de la universidad, en su casa, en su empresa; en fin, en

cualquier lugar donde haya un computador conectado a una red de información capaz de emitir y recepcionar señales de comunicación electrónica. La información producida y recepcionada por el usuario o internauta constituye el espejo de la realidad (realidad virtual), en tiempo real, concomitante o diferido, según factor *in témpore* en el que es recibida. Todo ello sin moverse físicamente del sitio de trasmisión o consulta de la información, pues el navegante electrónico es un caminante sin desplazamiento en el espacio geográfico.

Otro aspecto de forma externo del hipertexto, lo constituye la interactividad de los escritos, páginas WEB, y sobre todo, documentos electrónicos construidos con el lenguaje HTML. La interactividad posibilita al usuario enlazar documentos electrónicamente con cualquiera otro que guarde relación con aquél, no sólo como lo

---

(143) Normalmente se entiende por multimedia, a la utilización de los nuevos medios de comunicación basados en productos digitales o servicios que integran texto, gráficos, audio, película o vídeo, fotografía o animación, combinados con herramientas de software, los cuales permiten a los usuarios actuar de forma recíproca con estos. La multimedia puede presentarse en forma de productos de CD-ROM, en programas de ordenador ofrecidas en los kioscos, en servicios *on line* en los sitios de la red de redes de información mundial (WWW), y en las tecnologías de realidad virtuales. Vid. JARVLEPP, Harry. B.A., LL.B., M.B.A. *INFORMATION TECHNOLOGY AND NEW MEDIA LAW*. En: KnowledgeBase. An information Technology Law Bulletin- Fall 1997. En: WWW.UMONTREAL.EDU.CA.

(144) Citado por KATSH, *Ethain. RIGTHS, CAMERA, ACTION:... O*b. ut supra cit. En: WWW. UMONTREAL. EDU.CA.

hace el documento tradicional escrito con las referencias bibliográficas, citas de pié de página o remisiones internas o externas en un libro, sino y además, en forma dinámica, cuando puede consultar concomitantemente con el documento en pantalla las referencias bibliográficas, citas o remisiones en todo su contexto, y a la vez, las que aquél documento consultado refiere, y así sucesivamente en forma escalonada o gradual, hasta donde el interés del usuario-consultante se halle satisfecho (y muchas veces más allá) e ir a las mismas fuentes de producción de los documentos consultados por el enlace, sin importar el sitio geográfico donde se hallen, el tiempo horario real en el que se hace; el ambiente locativo en el que se halle (biblioteca privada o pública, siempre que no haya restricción al acceso electrónico); todo ello, con sólo identificar una dirección, ruta, camino electrónico (http:// WWW.,--http:**H**ypertext **T**ransfer **P**rotocol, es decir, la trasmisión de documentos electrónicos por hipertexto-- v.gr. Http:www.elcano.com. Buscador para páginas en español), o también conocido como *sitio en el WEB* o URL (**U**niform **R**essource **L**ocator) **[145]**.

Los vínculos **[146]** o enlaces electrónicos de un escrito o documento ibídem, pueden ser tantos como desee hacerlos el creador del documento, el usuario o consultante o el almacenador de la información. Los vínculos en una página WEB de hipertexto no sólo une documentos textuales, sino que también permite insertar imágenes fijas o de vídeo (formatos BMP), gráficos

en formatos GIF (***G**rafic **I**nterchange **F**ile*) o JPG (***J**oint **P**hotography **G**roup*) que potencian la presentación de documentos electrónicos e igualmente una amplia variedad de sonidos en diversos formatos (WAV, MIC, etc). Esa potencialidad de vinculación de multimedia y texto, se denomina *hipervículo* [147].

Los contenidos o aspectos de fondo del hipertexto son igualmente variopintos según el creador del documento y el sitio en el WEB, donde se hallen o consulten. A nuestros propósitos nos interesa los contenidos de las áreas jurídicas y lo que piensan los iusinformáticos al respecto.

4.3.2.5.1. EL S.O.S. DEL HIPERTEXTO EN EL DERECHO

El profesor *Ethain* [148], al comentar la importancia del *Nuevo Ambiente Tecnológico* generado por la información, la comunicación y la informática y en el cual

---

(145) TORBEN RUDOLPH, Mark. *TODO SOBRE*... Ob. ut supra cit., pág. 248
(146) Ibídem, pág. 264.
(147) KATSH, *Ethain. RIGTHS, CAMERA,:... O*b. ut supra cit. En: WWW.UMONTREAL.EDU.CA
(148) Ibídem.

hoy nos encontramos, hace énfasis en el hipertexto como la manera de comunicación electrónica entre juristas o profesionales de las ciencias sociales más idónea del presente y del futuro, puesto que las "nuevas tecnologías involucran y motivan a un creciente conocimiento que proporciona nuevas capacidades, oportunidades y experiencias" [149].

Joshua Meyrowitz, ha señalado que los medios de comunicación, como los sitios físicos, incluyen y excluyen a los participantes. Los medios de comunicación, como las paredes y las ventanas, pueden esconder o revelar. Los medios de comunicación pueden crear un sentimiento de participación y pertenencia o de exclusión y aislamiento. Por ello, se sugiere que las escenas físicas como las generadas por los medios de comunicación son parte de un todo continuo antes que una dicotomía. Lugares y medios de comunicación crean modelos fijos de interacción entre las personas, modelos fijos de flujo de información social [150] . Sin embargo, en la comunicación electrónica, los sitios físicos desaparecen y disminuyen las diferencias existentes en la interactividad de la comunicación formal o tradicional. El hipertexto es uno de principales prototipos de esta nueva realidad en crecimiento actualmente.

Los profesores *Saboy, Poulin y Choquette* [151] de la Universidad de Montreal (Canadá), han estudiado con detenimiento el impacto de los sistemas de hipertexto e hipermedia en el derecho, y especialmente en el campo de la investigación del derecho público, pues en esta área jurídica se manejan a diario grandes cantidades de documentos en la investigación que con los sistemas tradicionales hasta ahora seguidos significaría protuberantes desventajas frente a las

significativas ventajas que prodigan las nuevas tecnologías TIC y la informática, a través del hipertexto e hipermedia con todas sus potencialidades, funciones y características, tales como la interactividad de una gran cantidad de documentos electrónicos *on line* y *off line*, el acceso, consulta y transferencia de datos en formatos y velocidades electrónicas y la vinculación o enlaces con otros documentos que contienen texto, imágenes y sonido. Para ello, toman como prototipo el estudio y análisis de la *Loi sur l'assurance-chômage,* así como los cursos desarrollados en torno a esta.

Como siempre suele suceder al enfrentar un nuevo fenómeno que incide o impacta una área del conocimiento humano, y particularmente en el derecho, los investigadores siendo la voz silenciosa de muchos otros, se interrogan e intentan dar

---

(149) Ibídem.

(150) Citado por KATSH, *Ethain. RIGTHS,... O*b. ut supra cit. En WWW. UMONTREAL.EDU.CA

(151) Vid. SAVOY, Jacques (1); POULIN, Daniel (2) y CHOQUETTE, Martín.(1) *HYPERTEXTE EN DROIT: PROBLEMES ET DEFIS.* Département d´informatique et de recherche opérationnelle (1) y Centre de recherche en droit públic (2). Université de Montréal, Canada. En: WWW. UMONTREAL. EDU. CA.

plena contestación a la mismas. En el caso de los profesores canadienses, siguieron esta metodología al preguntarse: "*Existe-t-il un intérêt pour les hypertextes en droit*? **[152]** . En forma rotunda contestamos con ellos afirmativamente, no sólo por la gran cantidad de documentación producida por el derecho (normas jurídicas: leyes, decretos, Resoluciones, Directivas; obras jurídicas; providencias judiciales o administrativas; en fin.), sino por las múltiples ventajas que la informática jurídica esta brindando a la investigación del derecho por parte de los especialistas dentro de una nueva lógica y un ambiente nuevo que el profesor *Etain* denominó cultura electrónica, tal como antes lo comentamos. Así mismo por las características documentarias del derecho **[153]**, las cuales las podemos resumir así:

1. El empleo cada día mayor de grandes cantidades de información que sorprende a cualquiera, prueba de ello, por ejemplo en la Facultad de Derecho de la Universidad de Montreal, en su biblioteca cuenta con varios Bancos de datos: El Quicklaw con resúmenes de 100.000 decisiones de Tribunales; El Derecho Canadiense On line, contiene unas 350.000 resúmenes de decisiones, sin contar con otros, tales como el Banco de datos CanLaw, WestLaw, etc. Si estos bancos no se enlazan entre sí es muy difícil que sean consultados exhaustivamente por los juristas interesados en la investigación. Igual cosa sucede en todos y cada uno de los Estados modernos de derecho, en los cuales se produce una hiperexplosión de documentos provenientes del poder público (ejecutivo, legislativo y judicial), el Ministerio Público, la Defensoría del Pueblo (L´Ombusdman anglosajón) y en fin, ante cualquiera de las autoridades legitimamente instituidas en los Estados. 2. La consulta o la investigación de esta cantidad de información puede hacerse observando los índices o referencias que acompañan a los documentos que constituyen un

verdadero “hipertexto sobre papel”. Esto ocurre tanto en el aspecto legislativo, doctrinal y , sobre todo, judicial. A pesar de estas ayudas tradicionales, no es suficiente para el investigador. 3. Como sostiene *Bratley, P.* [**154**], el acerbo documental jurídico presenta hoy “*una dimensión evolutiva*”. Los cambios continuos en la documentación refleja la evolución del derecho. Las modificaciones son más o menos rápidas según las ramas del derecho, pero en todo caso, afecta a todos los sectores. La historia del derecho develada en los diferentes textos jurídicos muestra sucesivamente el verdadero “estado del derecho” (*l´état du droit*) durante su evolución. Todo lo cual conlleva el mejoramiento de los métodos y procedimientos de investigación de conformidad con los cambios evolutivos

---

(152) Ibídem.
(153) Ibídem.
(154) P. Bratley, D. Poulin, J. Savoy: *THE EFFECT OF CHANGE ON LEGAL APPLICATIONS*. Proceedings DEXA'91, Berlin (Germany), August 1991, 436-441. Citado por SAVOY, POULIN... Ob. cit. ut supra.

de las ciencia objeto de análisis y en especial, de las ciencias jurídicas; y, 4. La información documental jurídica es heterogénea. Esto quiere decir, que mientras la información legislativa tiene una lógica y plan preciso, no podemos afirmar lo mismo de la jurisprudencial que es producto de múltiples autores sobre distintas y puntuales controversias. De igual forma la doctrina tiene como fundamento diversas fuentes de investigación válidas y validables por sus autores y sus lectores. Esta heterogeneidad implica una ausencia de un vocabulario común y constante, una retórica estandarizada que debemos entender y analizar previa y concienzudamente.

Por todo ello, se impone para mejorar la consulta e investigación del derecho la implantación de un “sistema de hipertexto”. Sistema que conteniendo una parte tecnológica y jurídica previas, debe contener unos elementos esenciales para la construcción de una página WEB, una colección temática de estas; en fin, un sistema de hipertexto. Para su construcción se debe tener presente como elementos básicos los siguientes: a) Los Nudos; b) los Enlaces o vínculos, c) Las Rutas o Caminos y d) Las interfaces. Brevemente pasamos a explicarlos.

En primer término, debemos contar con los Nudos (“*Nodes o Noeuds*”) o unidades elementales y distintas de conocimiento o de información. El contenido de estos corresponde a un texto, un gráfico o una imagen. Estos contenidos pueden estar auxiliados por una voz digitalizada, una simulación, animación o una secuencia de vídeo. El término de hipertexto con estas ayudas se convierte en hipermedia, aunque cada vez por la utilización más común de la este último se han tomado como sinónimos: hipertexto e hipermedia, tal como antes se anotó. En el camino de transformación de una documentación en hipertexto, se debe trabajar los denominados nudos de tal forma que tomemos como ejemplo las divisiones lógicas de un texto (capítulos, subcapítulos, etc) para conformarlos. A cada nudo se le asigna un nombre o atributo formal

(nombre del autor, fecha de creación , etc). En el caso de la jurisprudencia, cualquier decisión es considerada un nudo, el atributo asignado serán los nombres de las partes, la fecha de expedición y demás datos que identifican a la providencia judicial.

En segundo término, *los enlaces o vínculos* ("liens o links") marcan la presencia de una relación entre dos nudos o entre dos partes de éste. Estos dirigen o envían a un lugar definido ("un carácter" o símbolo alfanumérico), a una zona ("serie de letras") o un nudo entero. En el hipertexto los enlaces o vínculos estructuran la infor mación, relievan las partes de un documento y marcan la división lógica de un escrito y además permiten exaltar la tabla de contenido, los índices o nudos referidos a éstos.

Por su parte, las rutas, caminos o "chemins o paths", constituyen una colección ordenada de enlaces o vínculos autorizados por el autor según criterios previamente determinados para que sean utilizados correctamente por el usuario o consultante de cierta información. La razón de ser de un sistema de hipertexto se fundamenta en la "invitación a utilizar como lo hiciera un explorador, las mismas fuentes de información en las que fue escrita una investigación" **[155]**. El ser humano puede de esta forma efectuar una lectura de un texto en forma más rápida utilizando sus capacidades intelectivas de una mejor y nueva forma y reconociendo fácilmente las fuentes, referencias, citas al instante.

Y finalmente, *la interface* de un sistema de hipertexto **[156]**, visualiza las partes en un documento, permite utilizar los desplazamientos hacia otros nudos relevantes o corrientes. De esta forma se amplia no sólo la opción visual de otros documentos, sino y además se potencia una de las características más importantes que tiene el hipertexto: construir documentos electrónicos "multifacéticos, multidimensionales y dinámicos, que incluyen texto, gráficos, animaciones y sonidos. Los enlaces o eslabones del hipertexto permiten unir documentos de un mismo servidor (o proveedor de información) como de cualquiera otro situado en el mundo. Así la información puede revisarse, consultarse o recolocarse en breves instantes con sólo pulsar un tecla" **[157]**, en forma digital o con el auxilio de unidades periféricas de salida o entrada de información (S/E) en un computador, en formatos y velocidades electrónicas sin moverse el usuario de su lugar de consulta.

Por tanto, hoy en día si un sistema jurídico informático documental de tipo instiucional, orgánico, universitario o estatal no cuenta con formatos, ambientes, estructuras y posibilidades de acceso, utilización y transferencias, a través de medios electrónicos y telemáticos basados en las ventajas del hipertexto o hipermedia, la probabilidad de evolución y cambio de las ciencias jurídicas en el milenio que se acerca serán mínimas, cuando no nugatorias que harán pedir a gritos un S.O.S. a quienes debieron implantarlos en sus diversos sistemas, sin eco posible.

5. EL PROCEDIMIENTO INFORMÁTICO, ELECTRÓNICO Y/O TELEMÁTICO DE DATOS PERSONALES.

5.1. CONCEPTUALIZACIONES TÉCNICO-JURÍDICAS DEVENIDAS DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) Y LA INFORMÁTICA JURÍDICA.

El rediseño de algunos conceptos jurídicos genéricos, como procedimiento,

---

(155) Ibídem.
(156) Ibídem.
(157) SIM, Peter. THE NEW ELECTRONIC DOCUMENT: A CHALLENGE FOR THE LEGAL SISTEM. Texto complejo: En: WWW.UMONTREAL. EDU.CA.

fases y principios y algunos otros específicos como procedimiento informático, electrónico o telemático; sistemas de tratamiento de entrada y salida (E/S) "automatizados de la información", "procedimiento de disociación", datos de carácter personal, "datos sensibles", etc., como se ha sostenido, han sido producto de la incursión en las áreas jurídicas de las llamadas nuevas tecnologías de la información y la comunicación TIC, en unión plena con la informática jurídica. En el presente aparte trataremos de conciliar ese rediseño conceptual, cuando menos, a los solos efectos de explicar el que llamamos procedimiento informático, electrónico o telemático, apoyándonos en el criterio de que los términos procedimiento, fases, principios, etc., no son instituciones jurídicas (procesales y sustantivas) propias y excluyentes de una rama del derecho, sino que están al servicio de las ciencias sociales por pertenecer a la teoría general del derecho [158], y por tanto, su utilización es patrimonio *erga omnes* y no *inter alios* en las ciencias jurídicas.

5.2. SISTEMAS DE TRATAMIENTO INFORMATIZADO Y EL PROCEDIMIENTO INFORMÁTICO DE DATOS.

La LORTAD al precisar lo que debemos entender por "*tratamiento automatizado*" (o mejor tratamiento informatizado, como se ha sostenido), siguiendo las directrices previstas en el Convenio de Estrasburgo de 1981 [159] y mas reciente- mente concretados por la Directiva 95/467CE [160], ha sostenido que tratamiento de datos ("automatizados" o no) esta constituido por el conjunto de "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".

De aquella conceptualización podemos deducir que el tratamiento por medios

---

(158) Mi trabajo. *LAS MEDIDAS CAUTELARES EN EL PROCEDIMIENTO ADMINISTRATIVO.* Universidad de Navarra (España), Junio 20 de 1986, pág. 456.

(159) "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),) Convenio Europeo de 1981.

(160) "*Tratamiento de datos personales* (´tratamiento´) : cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicados a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por trasmisión, 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),) . Directiva Comunitaria Europea 95/46/CE.

informáticos, electrónicos o telemáticos que permita una serie de funciones propias de los datos personales (recolección, grabación, etc.) endilgadas a conseguir unos fines o propósitos predeterminados por una persona privada o pública conforme a un ordenamiento jurídico vigente, podemos estructurar lo que ha de entenderse como procedimiento informático, electrónico o telemático de datos personales.

En efecto, entendemos por procedimiento informático de datos personales (género que incluye a la especie electrónico o telemático, en similar circunstancia a la conceptualización de datos personales informáticos, electrónicos o telemáticos, realizada al iniciar este aparte), aquél estructurado por una serie concatenada de etapas, fases o ciclos aplicables a los datos de carácter personal, de conformidad con el ordenamiento jurídico y apto para construir un fichero o banco de datos informatizados, o sistema estructural e informático de datos que permite ; entre otras atribuciones: el almacenamiento, consulta, difusión, cancelación, bloqueo o transferencia electrónica de datos.

Los *sistemas de tratamiento informatizado*, según el iusinformático *López Muñiz-Goni*[**161**], son aquellos de "carácter informático utilizados para establecer los criterios de búsqueda de los documentos", datos de cualquier tipo o informaciones, previamente a su recogida, selección, organización, estructuración, almacenamiento y registro, a través de medios informáticos, electrónicos o telemáticos. Estos sistemas apuntan a dos funciones que a la vez, constituyen una caracterización de uno y otro sistema. Estos son: Los sistemas de tratamiento informatizado de entrada y salida (E/S) de información. Estos apuntan al ingreso (input: I/) o la extracción (ouput:/O) información o datos estructurados informáticamente, constituyen la técnica metodológica idónea para recoger, almacenar y transferir datos o informaciones y cumplen funciones informáticas exclusivas de los ficheros o bancos de datos informatizados.

Los iusinformáticos como *López Muñiz-Goñi* [**162**] , han clasificado a estos sistemas

(161) LOPEZ MUÑIZ-GOÑI, Manuel. *INFORMATICA JURIDICA*... Ob. ut supra cit., pág. 71.

(162) En otro de nuestros trabajos hemos comentado los sistemas que el profesor López Muñiz-Goñi, clasifica de la siguiente manera: ***EL SISTEMA DE DESCRIPTORES*** (Thesauro jurídico). Toma como fundamento las palabras claves o "descriptores" que se utilizan para analizar un documento o una unidad in-formática siguiendo una serie de pautas lingüísticas, metodológicas e incluso cronológicas y de orden. Este sistema tiene un trabajo humano previo en su realización que no se puede considerar propiamente informático, sino manual, analítico, subjetivo, y muchas veces imperfecto. Por estas razones previas de elaboración, es por lo que el sistema tiene ventajas y desventajas. López Muñiz-Goñi, señala; entre otras:

desde el punto de vista formal y funcional. Por lo primero, los sistemas de tratamiento informático son de entrada y salida de información. Por lo segundo, hacen referencia a las funciones que los sistemas pueden tener, según sea sistemas basados en acceso o recuperación de información. Las funciones de los sistemas se fundamentarán en el textocompleto o "*full text*", en los "descriptores" (palabras claves organizadas en un thesauro) o en los resúmenes o "abstracts" de un texto. Todos estos sistemas tienen sus ventajas y desventajas que giran en torno al momento de elaboración (factor temporal), la subjetividad de los analistas o especialistas (más o menos acentuada, según el sistema escogido), la clase, calidad y cantidad de información o datos manejados y los costos sociales, económicos e intelectivos utilizados en la realización y puesta en funcionamiento de los sistemas de entrada/salida (E/S) de información.

Hoy en día, todos los sistemas de tratamiento informatizado de información emplean un sistema mixto tanto en el *input* como en el *output* de la información o los datos. En efecto, se utiliza sistemas de texto completo unido al de descriptores o sistemas de resúmenes unidos al de descriptores. Estos sistemas en su elaboración, diseño y estructuración tienen una previa parte manual o humana y otra exclusivamente informatizada [163], si se trata de "*tratamientos automatizados*" de información o datos, y será exclusivamente humano si se trata de tratamientos no automatizados. Esta aclara-

Continuación de cita No. 162

Como ventaja principal, la precisión en la búsqueda de la información requerida al trabajar con un número limitado de palabras claves. El inconveniente o desventaja, es la exigencia a la persona o analista de un trabajo concienzudo e intelectivo bastante especializado, según el área del saber humano que se trabaje. Los thesauros se clasifican así: 1. Según su estructura en: a) estructura arbórea horizontal, b) estructura arbórea vertical; 2. Por el idioma: a) Monolingüe, y b) Multilingüe; 3. Por su contenido: a) Monodisciplinares, b) Interdisciplinares; 4. Por la utilización Informatizada: a) Alfabético, b) numéricos; 5. Por la estructura lingüística: a) De descriptores, y b) Semánticos; 6. Por la forma: a) circulares, y b) Matriciales. ***SISTEMA DE TEXTO COMPLETO O "FULL TEXT".*** El sistema de texto integral o literal sirve para ingresar o recuperar información, en la misma forma y contenidos al de su incorporación o extracción. La salida de información se diferencia a la entrada no solo en el tiempo de acción por parte del analista o especialista o del usuario- consultor, según el caso, sino en la accesión a la información por las diferentes unidades periféricas computacionales de software o hardware utilizadas. En efecto las unidades (E/S) pueden ser: teclado, monitor, impresoras, mouse, etc. La información puede recuperarse también desde unidades de memoria central de un ordenador conectado *on line e incluso off line*, siempre que se disponga de los medios electrónicos o telemáticos idóneos. ***SISTEMA DE RESUMENES O "ABSTRACTS"***. Es aquél que combina los ventajas de los sistemas anteriores al realizar un sistema informático organizado por resúmenes enriquecidos de información que no suelen pasar de diez a quince renglones sobre los distintos textos analizados. A la vez utiliza un sistema de descriptores para poder ingresar y extractar información más rápidamente para el usuario. A pesar de unir ventajas sigue teniendo desventajas como la subjetividad de los analistas y un

margen de error más grande que el del texto completo al realizar resúmenes de textos no elaborados por ellos. Este sistema se utiliza mucho en materiales jurisprudenciales en todo el mundo. En la obra del autor citado y en nuestro trabajo un análisis más completo al respecto. *LA CONSTITUCION DE 1991 Y LA INFORMATICA*... Ob. ut supra cit., pág. 73 y ss.

(163) LOPEZ MUÑIZ-GOÑI, M., Ob. cit ut supra., pág. 39 y ss.

ción se hace, ya que la LORTAD, como las normas comunitarias europeas hacen referencia expresamente a estas dos clases de tratamientos de la información, y además, porque es nuestro propósito destacar que aún el sistema informático de tratamiento de datos tiene una parte inicial o *apriorística* de claro tinte intelectual o humano que es el que prepara, selecciona, estructura, organiza la información para meterla a un sistema informatizado. Trabajo humano previo que esta cargado de todas las ventajas y desventajas que esta clase de labores especializadas requiere, por ejemplo, para la elaboración de un sistema de tratamiento informatizado de información o datos jurídicos con documentación jurisprudencial, se requerirá de un grupo multidisciplinario conformado por lingüistas, iusinformáticos, ingenieros de sistemas, operadores, y sobre todo juristas, pues de lo contrario el sistema desde el punto de vista de la esencialidad de los contenidos estará muerto antes de nacer.

Ahora bien, el procedimiento informático de datos, siendo el género, *el procedimiento electrónico o telemático de datos* es una de las especies que se estructura por la utilización de medios y soportes informáticos electrónicos o telemáticos de software y hardware [164]. Desde el punto de vista iusinformático las funciones que cumple este procedimiento especial son las que la LORTAD determina como las de "cesiones de datos que resultan de las comunicaciones, consultas, interconexiones y transferencias", o en forma más explícita por la Directiva 95/46/CE, cuando hace referencia a que los "procedimientos automatizados, y aplicados a los datos personales... (en la) comunicación por trasmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión..." Como puede apreciarse el procedimiento electrónico o telemático de datos se utiliza básicamente en la trasmisión (emisión/recepción) de datos, y como tal, genera documentos, informaciones o datos de carácter electrónico o telemático que antes hemos comentado. Sin embargo, tanto el procedimiento genérico como el específico, tienen una misma estructuración en cuanto a las fases, ciclos o etapas, lo que los diferencia son las funciones que cada uno desarrolla en sistema de tratamiento informatizado. Sobre esto nos ocuparemos seguidamente.

5.2.1. FASES DEL PROCEDIMIENTO INFORMATIZADO DE DATOS.

El profesor *Morales Prats* [165], siguiendo al iusinformático *Frosini,* expone que en el *ciclo operativo de un sistema informático* (basado en el que se sigue para el estudio del *habeas scriptum* o habeas data), se distinguen las siguientes fases: a) Fase de

---

(164) Véase punto 2.4 y ss de esta parte y la parte IV de este trabajo.

(165) MORALES PRATS, Fermín. *LA TUTELA PENAL DE LA INTIMIDAD...* Ob. cit., pág. 65 y ss. Cita bibliográfica 125, capítulo I.

recogida de datos; b) Fase de tratamiento y programación de la información; c) Fase de conclusión del procesamiento de datos; y d) La trasmisión de la información. Esta última aunque *a priori* no la ubica como una de las fases del procedimiento informatizado de datos, luego sostiene que esta es una modalidad de "fase conclusiva del ciclo operativo" que incluso se puede subdividir así: a) cuando la circulación de datos se hace a través de un *circuito interno* de emisión (por medio de terminales de ordenador); o por *circulación externa,* que permite la divulgación de la información.

El autor citado, al comentar esta última modalidad de fase conclusiva del procesamiento de datos, hace recaer su importancia en que "la puesta en circulación de los datos materializa la dispersión de las informaciones de un individuo reunidas con anterioridad en el banco de datos y memorizadas de acuerdo al *software*. Este es el momento --agrega enfáticamente-- en que, potencialmente, pueden perpetrarse mayores atentados a la *privacy* de las personas; la libertad informática se traduce ahora en una auténtica *facultad de control* de la información personal, despojada de su carácter preventivo" **[166]**.

En nuestro criterio, siguiendo las pautas, metodología y criterios establecidos para los sistemas de tratamiento informatizados de entrada y salida (E/S) de información estudiados por el profesor *López Muñiz-Goñi,* referenciados anteriormente y las directrices normativas previstas en la LORTAD y las normas comunitarias: Convenio de Estrasburgo de 1981 y la Directiva 95/46/CE., hemos clasificado las etapas del procedimiento informatizado de datos así: a) Fase inicial o de *input,* constituida por la recolección y organización de datos. Fase que aún estando dentro del sistema informatizado es esencialmente producto de una actividad humana interdisciplinaria, según el área del saber humano que se maneje; b) Fase de tratamiento informatizado propiamente dicho o fase *in* de datos. En esta fase se inicia básica y esencialmente el procedimiento informatizado (llamado "automatizado" por la normativa española y europea) con toda su caracterización, funciones, elementos, soportes y medios informáticos, electrónicos o telemáticos; c) Fase de salida de datos o fase *output,* que a su vez, se subdivide en fase output general y fase output especial, según se utilicen medios informáticos, electrónicos o telemáticos *off line* u *on line.*

5.2.1.1. FASE INICIAL O *INPUT*: RECOLECCIÓN, SELECCION Y ORGANIZACIÓN ESPECÍFICA DE DATOS.

---

(166) Ibídem, pág. 70 y ss.

Esta etapa en cualquier sistema informatizado se lleva a cabo con mecanismos, metodología e instrumentalizaciones de carácter humano, aunque no se descarta que parcialmente se realice con soportes y medios informáticos, electrónicos o telemáticos, una vez han sido recolectados los datos manualmente, tras la aplicación de encuestas, entrevistas, volantes, cumplimentación de formularios o impresos, etc. Es decir, que se recoge la información o datos con medios manuales para posteriormente seleccionar y organizarla con medios informáticos, con programas de ordenador y hardware idóneos para la realización de dichas labores. Sin embargo, no se descarta que en algunas disciplinas del saber humano y en la formación de ciertos ficheros o bancos de datos (v.gr. con carácter estadístico, archivístico, histórico, científico e investigativo en sociología, economía, ingeniería e incluso en derecho), la recolección de información o datos se realice por completo con medios informáticos de software y hardware, por cuanto la información se halla almacenada en memoria central o periférica de un ordenador *off line* u *on line*. En este último se descarta la actividad de inmediatez humana directa y personal y se reemplaza por la realización humana indirecta a través de medios informáticos.

La parte de esta fase realizada con medios y recursos de carácter humano tiene como características principales la de ser una actividad humana, especializada, personal o por regla general de carácter colectivo y multidisciplinaria, según el tipo, cantidad y calidad de información o datos recogidos. Esta parte, con todas sus ventajas o desventajas constituye una parte de la fase inicial de carácter subjetivo, bien se haya realizado directa y personalmente o en forma indirecta con medios informáticos.

Como lo sostiene el profesor *Morales Prats* [**167**], durante este período se presentan los mayores problemas para el legislador; entre otros, los surgidos en torno a la fijación de los límites de la licitud de las recolecciones de datos. Como principio general debe propugnarse la *prohibición* de la recogida de los *datos sensibles*, cuyo procesamiento puede atentar la intimidad de las personas y en consecuencia posibilita prácticas discriminatorias; son informaciones que revisten esta calidad: los datos relativos a la raza, opciones religiosas, filiación política, actividades sindicales, hábitos sexuales, antecedentes judiciales, así como historiales sanitarios, entre otros. Esta prohibición debe estar por encima incluso de un eventual consentimiento del titular de la información o datos, y el cual sólo será permisible para la recolección de información de "carácter personal no sensible", aunque el legislador deberá regular en forma "casuista", cuales se consideran tal.

---

(167) Ibídem, pág. 70 y ss.

El Convenio de Estrasburgo de 1981, enfáticamente al categorizar las clases de datos personales sostuvo que los datos de carácter personal 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, no podrán tratarse automáticamente *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). Esta norma europea extiende este principio de prohibición de recolección de datos conocidos como del *"núcleo duro de la privacy"*, según el derecho anglosajón, como una regla general; pero establece una ventana de excepción a la prohibición, cuando sostiene que las legislaciones estatales podrán regular el tratamiento informatizado de aquellos datos si el ordenamiento jurídico previere específicamente medidas de protección y garantías apropiadas. Sin embargo, dicha excepción no se establece para los datos personales referidos a *condenas penales* (parte *in fine* del artículo citado).

La LORTAD (L.O. 5/1992, Oct. 29), en el marco del ordenamiento jurídico español al reglamentar el art. 18.4 de la CE., toma como referente la ventana de excepción del Convenio Europeo, para establecer una categorización de datos personales según los niveles de protección referidos a cada una de estas. Así establece una clase de "datos especialmente protegidos" (art. 7) y dentro de aquellos los subdivide así: a) Los datos relativos a la ideología, religión y creencias, según el art. 16-2 CE, nadie esta obligado a declarar en contra de aquellos, sólo podrán ser recolectados (o "recabados"), si existe consentimiento del titular, previa la admonición o derecho de información, de su "derecho a no prestarlo"; b) Los datos relativos a la ideología, religión y creencias, "podrán ser objeto de un tratamiento automatizado de datos de carácter personal", con el consentimiento expreso y por escrito del titular de los mismos ("el afectado" dice indebidamente la norma). Aquí se permite no sólo la fase inicial del tratamiento informatizado, como en los datos personales del literal anterior, sino para todas las fases del procedimiento en esta categoría de datos; c) Los datos personales referidos al origen racial, a la salud y a la vida sexual "sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo dispongan una ley o el afectado consienta expresamente" (art. 7-3). Se permite el tratamiento informatizado en todas las fases del procedimiento, aunque hace énfasis en la etapa inicial y última del procedimiento, especialmente la referida a la trasmisión de datos por "cesión"; d) Los datos personales relacionados con la ideología, religión, creencias, origen racial o la vida sexual y hayan sido objeto de tratamiento informatizado en todas sus fases quedan "prohibidos" si su "finalidad exclusiva" radica en el "almacenar" estos datos (art. 7-4). Aquí se prohíbe no la recolección de esta clase de datos con carácter informático, sino el almacenamiento en memoria central o periférica de los datos tratados informáticamente; y, e) Los datos de carácter personal relacionados con la "comisión de infracciones penales o administrativas" , sólo podrán ser tratados informáticamente, sí el ordenamiento jurídico vigente sobre la materia lo permite. Esta dispensa legal para el tratamiento informático, excluye cualquiera otra. Sin embargo, la LORTAD en esta temática, utiliza indebidamente la terminología iusinformática, pues hace referencia a una posible "inclusión" en "ficheros automatizados de las

Administraciones Públicas competentes" de datos relativos a la comisión de infracciones penales o administrativas, cuando lo que debe aclarar es si pueden ser o no objeto de tratamientos informatizado, a partir de qué fase o fases y hasta cuáles otras se extiende la prohibición o permisión, si fuere el caso.

Por su parte, la Directiva Comunitaria 95/46/CE, establece una regla general y amplia gama de excepciones sobre la prohibición para todo el tratamiento informatizado de categorías especiales de datos personales que revelen el 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). La Directiva no hace distinción ni en el nivel ni en los requisitos exigidos para la protección de las diversas categorías de datos personales, como sí lo hace la LORTAD. Sin embargo, establece una serie de excepciones a la regla general, como es usual en la normativa comunitaria, que en nuestro criterio hace casi nugatoria la regla.

A título enunciativo veamos algunas de las excepciones. Estas son: a) Cuando haya dado su consentimiento explícito a dicho tratamiento, salvo que la legislación de los Estados miembros de la CE., disponga que la prohibición no puede levantarse aún con el consentimiento del titular de los datos; b) 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 éste prevea garantías adecuadas; c) 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; d) El tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una 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; e) El tratamiento se refiere 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 (art. 8-2, literales (a), a (e),) .

Se establece también en la norma comunitaria, unas excepciones de carácter especial, según se trate de datos personales de carácter médico; por motivos de interés público; o bien, se refieran a datos relativos a infracciones, condenas penales o medidas de seguridad, sanciones administrativas o procesos civiles (art. 8-3 a 5). En estos casos previo el lleno de unos requisitos de forma y de fondo, tales como: a) para el caso de datos personales médicos, se requiere que 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 un 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; b) En el caso de datos personales, por "motivos de interés público importantes", podrán ser sujetos de tratamiento, con las excepciones previstas en los literales (a), a (e) del art. 8-2 de la Directiva 95/46/CE, o las que establezca el derecho interno de los Estados miembros, o bien por una autoridad de control de los poderes públicos (jurisdiccional o administrativa); y, c) En el caso de los datos personales relativos a infracciones, condenas penales, medidas de seguridad, sanciones administrativas o procesos civiles, podrán ser objeto de tratamiento cuando se realicen "bajo el control de la autoridad pública" o si el derecho interno de los Estados miembros prevén garantías apropiadas y específicas. Sin embargo, para el caso de las condenas penales, podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. En los casos anteriormente previstos en los literales b) y c), los Estados miembros de la CE, "notificarán a la Comisión" creada al efecto por la Directiva.

Una especial consideración de la Directiva, le dedica al tratamiento de datos personales y la "libertad de expresión", cuando permite dicho tratamiento, siempre y cuando sea con fines exclusivamente periodísticos o de expresión artística o literaria, llamando la atención a los Estados miembros para que establezcan "exenciones y excepciones", en la medida que resulten necesarias para "conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión" (art. 9). Exenciones y excepciones, que en la Directiva constituyen una variada gama, como anteas apenas si hemos enunciado (sobre los capítulos III. IV y VI).

Una directriz general que establece la Directiva Comunitaria aplicable no sólo a la fase inicial del tratamiento informatizado sino durante toda la existencia de éste es como sigue: los datos recogidos con "fines determinados, explícitos y legítimos", 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 oportunas" (art. 6-b,).

Ahora bien, sea que se permita el tratamiento informatizado de datos personales y dentro de estos los denominados "sensibles" (caso LORTAD), o bien se permita el tratamiento de datos personales por vía de excepción (caso de las normas comunitarias: Convenio y Directiva), o más aún se permita dicho tratamiento, porque así esta previsto en el ordenamiento jurídico vigente comunitario o nacional (caso de España), el titular de los datos personales sometidos a tratamiento tendrá una enriquecida serie de derechos, pero también deberes que cumplir.

En efecto, estos derechos y deberes surgen *ipso jure* con el sometimiento de un dato personal a un procedimiento informatizado.

No pretendemos agotar en este aparte el tema, que por demás ha sido objeto de estudio concienzudo y amplio en el derecho privado español v.gr. *Orti Vallejo* [168] y *López Díaz* [169] , sino destacar esos aspectos importantes de la visión iusinformática de la intimidad, en armonía con los principios de protección de los datos personales cuyo tratamiento ha sido mediante medios informáticos, electrónicos o telemáticos.

En efecto, en el Título II de la LORTAD, bajo el nomen de "Principios de la protección de datos", se recogen principios propiamente dichos, derechos (como el de *habeas data* en toda su extensión: acceso, actualización, rectificación, cancelación o borrado de datos y el *derecho a la información*, a los que nos referimos en la parte IV del trabajo y que son objeto específico del Título III, LORTAD) y obligaciones de los sujetos intervinientes (v.gr. El ejercicio de las acciones pertinentes en caso de falleci miento del interesado; las del responsable del fichero; la gestión del fichero por un tercero por cuenta del responsable del fichero, etc) en el tratamiento de datos por medios informáticos, electrónicos y telemáticos, con lo cual el contenido no se compadece con la rúbrica; más aún, constituye una rémora que arrastra la LORTAD del Convenio del Consejo de Europa, posteriormente reiterada por la Directiva 95/46/CE, e incluso contiene una avalancha de excepciones a los principios de protección de datos que en momentos los hacen nugatorios, o cuando menos, los dejan tan endebles que

---

(168) ORTI VALLEJO, Antonio. *DERECHO A LA INTIMIDAD E INFORMÁTICA*. Ed. Comares, Peligros (Granada), Esp., 1994, pág.71.

(169) LOPEZ DIAZ, Elvira. *EL DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD*. -- Jurispru prudencia y doctrina--. Ed. Dykinson, Madrid (Esp.), 1996, pág.169 y ss.

parece no existieran en la ley como candados de protección, pues cualquier llave o algo que se le parezca los abre. De ahí que se hayan presentado diversas demandas de inconstitucionalidad ante el Tribunal Constitucional Español que desde 1994 esperan resolución [170].

Entre muchas otras clasificaciones, destaquemos la del profesor *Davara* [171], el cual los clasifica, así: a) Pertinencia de los datos, b) El derecho de información de los afectados de modo expreso, preciso e inequívoco, c) El consentimiento, salvo que la Ley disponga otra cosa, d) La Cesión de los datos. Por su parte, *Souvirón* [172], agrupa a los principios, así: a) De congruencia y racionalidad, b) Transparencia, c) Calidad y veracidad de los datos almacenados, d) El consentimiento o de autodeterminación del "afectado", diferente si son datos personales de carácter general o se trata de datos denominados "sensibles", e) Seguridad de los datos; y , f) El Principio del Secreto.

Ahora bien, teniendo en cuenta que los principios no son meras declaraciones pragmáticas establecidas por el legislador, sino contenidos axiológicos que sirven a unos fines u objetivos de la materia objeto de la misma ley y que por esto son de la esencia en la interpretación o hermenéutica jurídica de los asuntos relacionados. En otros términos, son contenidos de esencia, presencia y decisión de un continente o materia específica. En nuestro caso, los principios de protección de los datos persona les deben revelar esos contenidos de esencia, presencia y decisión en las fases del procedimiento de tratamiento por medios informáticos, electrónicos o telemáticos de los datos, pues es hacia ahí donde estan orientados rectamente estos principios, no hacia los derechos y deberes de los sujetos intervinientes en el procedimiento, pues estos tienen su estructura propia delimitada por la misma LORTAD, aunque obvia y finalmente los implique, tal y como veremos más adelante.

En tal virtud, en la *fase inicial de recolección, selección y organización de los datos personales*, deben imperar una serie de principios que involucran a la licitud, calidad, cantidad, oportunidad, proporcionalidad, compatibilidad con los fines de los datos mismos y de información. En este sentido, la LORTAD, establece que los datos

---

(170) En la parte final de la primera parte de éste trabajo nos referimos a este punto. Aquí nos dedicaremos a describir los que se consideran estrictamente principios de protección de los datos personales.

(171) DAVARA R. Miguel A., *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi S.A., Pamplona, 1997, pág. 33

(172) SOUVIRON, J.M. *EN TORNO A LA JURISDICCION DEL PODER INFORMATICO DEL ESTADO Y EL CONTROL DE DATOS POR LA ADMINISTRACION*. En: Revista Vasca de Administración Pública. R.V.A.P. No. 40, Ed Arailla, Arendua, Sep-Dic., 1994, pág. 34.

deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se haya obtenido (art.4.1). Estas finalidades que deben perdurar hasta las fases de almacenamiento, conservación y utilización de los datos (Exposición de Motivos y art.4.2. LORTAD).

En la E.de M. de la LORTAD, ha quedado patentizado estos argumentos cardinales, así:

> *Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandado constitucional, se pretende limitar*.

Igualmente, atendiendo al consentimiento de forma inequívoca dado por el interesado en el momento de la recogida de datos y por las subsiguientes fases del procedimiento y cuya "base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita" (E de M., LORTAD) [173], el interesado deberá ser previamente informado de modo expreso, preciso e inequívoco de una serie de actividades, facultades y derechos (constitucionales --art. 16.2 CE-- o, legales --art.5 a 8-- LORTAD) que le conciernen como sujeto titular, identificado o identificables (*cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de una persona*) de los datos, mismos que se abordan al final de esta parte del trabajo.

Actividades previas y derechos tales como: 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 el *habeas data y*, e) De la identidad y dirección del responsable del fichero. De igual manera, a exigir que los cuestionarios u otros impresos utilizados para la recogida, sean claros, precisos y con las advertencias pertinentes al caso (art. 5.1 y 5.2 LORTAD)

En el Convenio Europeo de 1981, en iguales términos determina la mencionada serie de principios para esta fase inicial del procedimiento, bajo el intitulado de "Calidad

---

(173) Texto completo en: AA.VV. DISCOS COMPACTOS ARANZADI... Ed. Aranzadi, 1998.

de los datos" (art. 5) y "Categorías particulares de datos" (art. 6), haciendo énfasis en que los datos se obtendrán y tratarán leal y legítimamente, serán exactos y si fuere necesario puestos al día y queda prohibido la recolección como cualquier tratamiento "automatizado" de datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos relativos a la salud, a la vida sexual o los referentes a las condenas penales.

En la Directiva 95/46/CE, divide estos principios de la fase inicial del procedimiento en los principios relativos a la "calidad de los datos" y los principios relativos a la "legitimación del tratamiento de datos". Entre los primeros destaca que los datos personales objeto y sujetos a tratamiento informatizado por parte de los Estados miembros, al menos en la fase inicial del procedimiento se tendrá en cuenta que estos datos serán tratados así: a) de manera leal y lícita, b) recogidos con fines determinados, explícitos y legítimos, c) ser adecuados, pertinentes y no excesivos a los fines para los cuales se recogen ("recaban"), d) ser exactos, y cuando sea

necesario, actualizados, e) recogidos y conservados en una forma que permita la identificación de los interesados.

En los principios relativos a la legitimación del tratamiento de datos, establece unos derechos-deberes para los titulares de los datos, así como una serie de garantías para los Estados miembros que deben implementar cuando un dato personal se someta a procedimiento informatizado. El titular de los datos o "interesado" como le llama la Directiva, permitirá el tratamiento informatizado de datos personales, siempre que: a) haya dado su consentimiento de forma inequívoca; b) sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; c) sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) sea necesario para proteger el interés vital del interesado; e) 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 los datos; y, f) 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 requieren protección, en particular el derecho a la intimidad (art.7 en conc. art. 1-1, Directiva).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* [174], establece

---

(174) Texto completo en: WWW.UMONTREAL.EDU.CA.

una serie de principios aplicables a las diferentes fases del procedimiento informatizado que hemos planteado. En efecto, el art. 21, consagra como primer principio el de "La manera y propósitos de la recolección de la información", en éste se establece que la información personal no debe ser coleccionada por una personal natural o jurídica (institución, entidad o corporación) privada o pública, para la inclusión en un registro informático (fichero o banco de datos) o en una publicación generalmente disponible a menos que : a) la información sea reunida para propósitos legales directamente relacionados con una función o actividad del propias del recolector de la información o coleccionista; y , b) la recolección de la información sea necesaria para cumplir con los propósitos señalados. En todo caso, la información o datos personales no deben ser recogidos por medios ilegales o injustos.

5.2.1.2. FASE DE TRATAMIENTO INFORMÁTICO PROPIAMENTE DICHO O FASE *IN* DE DATOS. EN ESPECIAL, EL ALMACENAMIENTO, EL REGISTRO Y LA CONSERVACIÓN DE DATOS PERSONALES.

Si bien el tratamiento informático comienza con la recolección, selección y organización de la información, la fase propiamente informática inicia, por regla general, en la presente fase, la cual hemos denominado *fase in de datos;* o una vez, que se disponga de un software y hardware apropiados para el tratamiento informatizado de los datos personales, la fase es *in tótum* ***IN****formática de datos.*

Esta fase se subdivide, a su vez, en otras subetapas necesarias para el pleno desarrollo del tratamiento informático de los datos personales. Estas son: almacenamiento en memoria central o periférica de ordenador (storage), el Registro Informático (visión iusinformática y iusadministrativa), y la conservación de datos (jurídica y tecnológicamente) que implica no sólo el mantenimiento sino la administración de los datos, según su origen y fines para los que fueron recolectados, almacenados y registrados por los responsables (públicos o privados) de los mismos.

La aclaración del inicio propiamente informático obedece a la advertencia hecha en la anterior fase sobre la actividad esencialmente humana del procedimiento, salvo que se realice con datos personales con fines exclusivamente estadísticos, históricos, científicos, investigativos, archivísticos o de cualquier otro género parecidos que se hallen almacenados en memoria central o periférica de un ordenador o sea producto de trasmisión o teletrasmisión (emisión/recepción) de datos, con similares fines. En consecuencia, la fase inicial del tratamiento puede ser exclusivamente humana o tecnológica o informática o mixta. En cambio, esta fase es exclusivamente tecnológica o informática, pues los datos ya recogidos, seleccionados y organizados son objeto directo de tratamiento por software o hardware idóneos con soportes y medios informáticos, electrónicos o telemáticos.

Ciertamente, como afirma el profesor *Morales Prats* [175], los requisitos para un tratamiento de los datos, controlado y con garantías, se centran, por un lado, en la adopción de medidas de seguridad técnicas que preserven los datos adquiridos de accesos ilícitos y de fugas de información y, por otro lado, en el mantenimiento de la transparencia durante el proceso hasta la obtención de los resultados de programación (software). Sin embargo, también debe implementarse medidas no sólo que aseguren los datos personales *per se* sino que también garanticen los derechos y deberes de los titulares de los mismos, a la vez, que potencien las garantías sustantivas y procesales por parte de los Estados en sus respectivos ordenamientos jurídicos. A fin de analizar estos aspectos en su conjunto pasamos a analizar las subetapas de esta fase.

5.2.1.2.1. EL ALMACENAMIENTO ELECTROMAGNETICO DE DATOS PERSONALES.

Almacenar datos personales, al menos a los fines de este trabajo, consiste en guardar electromagnéticamente datos digitales (texto, sonido e imágenes) con y en soportes y medios informáticos, electrónicos o telemáticos de software o hardware (en forma provisional o definitiva), datos considerados personales por el ordenamiento jurídico, aptos de ser objeto y sujetos de tratamiento informatizado, a fin de que cumplan los propósitos legales y legítimos previstos desde del inicio del tratamiento informatizado conforme lo autoriza el ordenamiento jurídico o autoridad competente.

El almacenamiento de datos personales constituye por tanto, una actividad tecnológica de carácter informática con soportes y medios igualmente informáticos configurada por esta parte eminentemente tecnológica (software y hardware idóneos); y otra, de índole jurídica. Tecnología y derecho interactúan de forma plena en un marco de almacenamiento lícito, legítimo y ajustado a los requerimientos tecnológicos. Aquí haremos énfasis en aspecto jurídico.

El almacenamiento electrónico de datos, en soportes y medios de hardware, sea en forma provisional (en memoria central del ordenador) o sea en forma definitiva (en el *hard disk del ordenador*, discos flexibles, discos compactos, o unidades de "backup" –

---

(175) MORALES PRATS, Fermín. *LA TUTELA*.... Ob. cit. pág. 67-68.

copias de seguridad--), se realiza en formatos, velocidades y lógica de ordenación de datos o información con carácter electromagnético, por ser una de las principales funciones de todo sistema, equipo o dispositivo de computador. El almacenamiento de datos en *el hard disk*, como uno de los dispositivos más importantes de entrada y salida (E/S) de información, lo es, porque en términos de *Norton* [176], es una especie de "biblioteca de referencia del ordenador, centro de clasificación y caja de herramientas, todo en uno".

El almacenamiento de datos, en soportes y medios de software o programas de computador tecnológicamente siguen los mismos pasos de E/S de información que para los soportes y medios de hardware, tanto en forma provisional como definitiva, con la diferencia de que en éstos el almacenamiento es de carácter logicial o intangible y en aquéllos de carácter material o físico [177].

Almacenar electromagnéticamente datos de cualquier índole, descarta la simple acción de almacenamiento indiscriminado, ilegítimo e ilegal, sin parámetros de la lógica electrónica (que incluye potencialidades y funcionamiento electrónicos posteriores para un usuario de un fichero o

banco de datos), tal como si fuese un gran armario donde se guardan cosas, elementos, papeles o documentos continentes de datos y a los cuales puede acceder cualquier persona en el momento que les plazca. Es decir, se descarta aquellos armarios o "ficheros o banco de datos" que en concepto de *Fairen Guillén* [178], son simples "*almacenes de datos"*, en donde la "menor indiscreción --perdónese la palabra, aquí no demasiado adecuada-- puede producir la ruina del honor, de la familia, de la intimidad del ciudadano", puesto que no es una visión iusinformática del término almacenar la que se vierte y entiende con aquél concepto, sino una visión gramatical aplicada por deducción al *storage electrónico.*

Para entender el *storage electrónico*, debemos partir de la lógica del mundo escriturario o de la impresión y luego adentrarnos en la lógica electrónica (según el profesor *Ethain*), pues almacenar datos electrónicamente no sólo es apilar, guardar o compilar información o datos como papeles o documentos en un armario, sino que almacenar (como fenómeno electromagnético) incluye además actividades; tales como:

---

(176) NORTON, Peter. *EL IBM PC A FONDO.* Técnicas de programación avanzada (" Inseide The IBM: Acces to avanced features and programming). Trad: José Antonio Daza. Ed. Anaya, Madrid, 1987, pág. 29 y ss.

(177) Ibídem, pág. 29 y ss.

(178) FAIREN GUILLEN, Víctor. *EL HABEAS DATA Y SU PROTECCION ACTUAL SURGIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992*. En: Revista de Derecho Procesal. Editoriales de Derecho Reunidas, S.A., Madrid, 1996, pág. 529

la organización en memoria del ordenador (sea por fecha de creación, por extensión del archivo o *file*, en orden alfabético, en orden ascendente o descendente, etc); seleccionar, estructurar (según entrada de archivos, programas base o aplicativos, por jerarquía en el árbol de directorios, subdirectorios, --*The Tree*--, etc); enlistar o encaminar (seguir un *path)* y proporcionar *a posteriori,* en el acceso a aquéllos datos, una información en formatos y velocidades igualmente electrónicas. Quizá por esta versatilidad en las posibilidades y funciones de los datos almacenados electromagnéticamente, es por lo que no puede seguirse pensando en el término almacenar como sinónimo de arrumar o apilar sino que debemos sintonizar el término con el fenómeno iusinformático y lo que ello engendra, cuando menos, en el mundo del derecho.

El *storage electrónico* en memoria central y periférica de un ordenador de los datos personales, sea cual fuere el *programa o software-base* [179] que se utilice, junto a los *programas-aplicativos* [180], deben reunir los requisitos técnicos preestablecidos por la autoridad, institución, entidad u organismo encargado de aplicarlos, a fin de cumplir con los propósitos legales, lícitos, legítimos y justos *a priori* perseguidos con el mentado tratamiento. Estos requisitos están previstos en el ordenamiento jurídico para homologar, estandarizar; y en fin, generalizar la aplicación y utilización de estos medios tecnológicos conforme a derecho. En la legislación española, por ejemplo, se ha iniciado con la regulación de la utilización de soportes,

medios y aplicaciones informáticas, electrónicas y telemáticas en el sector público [181], lo cual no obsta para extender su aplicabilidad al sector privado, pues la LORTAD, proporciona facultades de control

---

(179) MORALES P., Fermin. *LA TUTELA PENAL DE LA INTIMIDAD.... Ob.* ut supra cit., pág. 67-68.

(180) Ibídem.

(181) AA.VV. *DISCOS COMPACTOS ARANZADI*. REAL DECRETO 16-2-1996, núm. 263/1996. PUBLICACIONES: BOE 29-2-1996, núm. 52, [pág. 7942] Regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. *Artículo 2. Derechos de los ciudadanos y limitaciones*.1. La utilización de las técnicas señaladas en el artículo anterior tendrá las limitaciones establecidas por la Constitución, la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos. En especial, se garantizará el honor y la intimidad personal y familiar de los ciudadanos ajustándose, a tal efecto, a lo dispuesto en la Ley Orgánica 5/1992, de Regulación del tratamiento automatizado de los datos de carácter personal, y en las demás Leyes específicas que regulan el tratamiento de la información así como en sus correspondientes normas de desarrollo. La utilización de tales técnicas en ningún caso podrá implicar la existencia de restricciones o discriminaciones de cualquier naturaleza en el acceso de los ciudadanos a la prestación de servicios públicos o a cualquier actuación o procedimiento administrativo. 2. Cuando la Administración General del Estado o las entidades de derecho público vinculadas o dependientes de aquélla utilicen técnicas electrónicas, informáticas y telemáticas en actuaciones o procedimientos que afecten de forma directa o indirecta a derechos o intereses de los ciudadanos, se garantizará la identificación y el ejercicio de la competencia por el órgano correspondiente. En este supuesto, los ciudadanos tendrán derecho a obtener información que permita la identificación de los medios y aplicaciones utilizadas, así como del órgano que ejerce la competencia.

técnico-jurídico a instituciones con un régimen y representatividad jurídicas *sui géneris* (puestos en evidencia por inconstitucionalidad, ante el Tribunal Constitucional Español [182]), conocido como la Agencia de protección de Datos.

La LORTAD, las normas comunitarias, y en general, las normas sobre datos personales sometidos a tratamiento informático, electrónico o telemático, han puesto mucho énfasis en esta subfase de la etapa input de datos, pues como lo sostiene la LORTAD en la E.de M., "*el progresivo desarrollo* de las técnicas de recolección y *almacenamiento de datos* y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida". Amenaza que unida al avance de las tecnologías de la información y de la comunicación (TIC), que "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" [183].

Como fundamento primigenio de protección y garantía de los derechos y libertades públicas de los titulares de datos personales, almacenados en ficheros o bancos de datos, ha instituido, "el principio de consentimiento, o de autodeterminación", por medio del cual el titular

es consciente de sus actos, hechos u omisiones referentes a los datos personales que ha entregado, y a la vez, esta informado plenamente de aquellos que han sido recolectados [184] y almacenados por su propio querer de conformidad con el ordenamiento jurídico y/o autoridad competente. Por ello, en la E.de M., de la LORTAD, se afirma que la protección de los datos personales " se refuerzan singular-

---

(182) Véase, la aparte in fine de la parte I, de este trabajo.

(183) Texto completo en: AA.VV. DISCOS COMPACTOS ARANZADI S.A.

(184) "*Artículo 5. Derecho de información en la recogida de datos.* 1. Los afectados (por titulares de datos) a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: 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. e) De la identidad y dirección del responsable del fichero. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.3. 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". Texto completo en: AA.VV. DISCOS COMPACTOS ARANZADI S.A.

mente 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" [185].

Con base en estas previsiones de claro tinte proteccionista, así como las sostenidas por el Convenio Europeo de 1981, sobre la materia, y también las contenidas en la CE (art. 10), la LORTAD, pone más énfasis en algunos de los datos personales considerados parte del *núcleo duro de la privacy*, cuando sostiene: "quedan prohibidos los ficheros creados con la finalidad exclusiva de *almacenar datos de carácter personal* que revelen la ideología, religión, creencias, origen racial o vida sexual". (art. 7-4), aunque los otros no es que se excluyan por deducción, como pudiera pensar *apriorísticamente*, pues estos quedan tácitamente incluidos dentro de la prohibición mentada cuando hace referencia al tratamiento informatizado de los datos, pues el almacenamiento, como hemos sostenido hace parte de ese tratamiento.

Por su parte la Directiva 95/46/CE, establece un cuadro de protección genérica del procedimiento informatizado de datos dentro del cual se incluye la subfase de almacenamiento. En efecto, la norma sostiene: " los principios de protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios" (Considerando 68); es decir, a los principios relativos a la calidad de los datos (art.6) y a los principios referidos a la legitimación del tratamiento de datos (art. 7), que hacen referencia a la licitud y legitimidad de los tratamientos de datos personales, antes enunciados según los parámetros de la LORTAD.

Sin embargo, cabe resaltar el Derecho a la información que tiene el titular de los datos cuando estos sean recabados del propio interesado, o incluso cuando no han

---

(185) Agrega la E.de M., que "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 (por titular de los datos), 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". Texto completo en: AA.VV. DISCOS COMPACTOS ARANZADI S.A.

sido recolectados de éste, no sólo en el momento de la recolección de los mismos, como viene siendo estudiados y exaltados, por la doctrina [186] sino, y por sobre todo en el momento del almacenamiento de los mismos, pues es aquí donde se genera como surtidor, tanto el cuadro proteccionista o garantísta de los derechos o libertades públicas por los Estados, como los posibles y gamados métodos de desconocimiento y vulneración de aquéllos, y por tanto, conviene enfatizar unos y otros en esta subetapa del proceso informático, máxime cuando la recogida de datos ha sido eminentemente informática, puesto que diferente es el caso si la recolección de datos es total o parcialmente humana, como antes hemos visto.

En efecto, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar al titular de los datos personales que le conciernan, lo siguiente: a) la identidad del responsable del tratamiento, o de su representante, según fuere el caso; b) los fines del tratamiento de que van a ser objeto los datos; c) la información sobre los destinatarios o las categorías de destinatarios de los datos; d) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder; e) la existencia de derechos de acceso y rectificación de los datos que la conciernen, si fuere del caso (art. 10 Directiva.)

El Derecho de información cuando los datos no han sido recolectados del propio interesado, se hace efectivo así: Los Estados miembros dispondrán que el responsable o su representante deberán, desde el momento del registro de los datos o, en caso de que se 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 información siguiente, a menos que ya hubiese sido informado (Esto no se aplicará en el caso del tratamiento de datos con fines estadísticos o de investigación histórica o científica [187]). Estos son: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que va a ser objeto los datos; y

en fin, los mismos otros derechos que tiene el titular de los datos cuando han sido recogidos del propio interesado (Artículo 11).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* [188], establece una serie de principios aplicables a las diferentes fases del procedimiento informatizado.

---

(186) ORTI VALLEJO, Antonio. *DERECHO A LA INTIMIDAD E INFORMATICA... Ob*. cit., pág. 136 y ss. Los autores allí citados. v.gr. Albadalejo, Diez Picaso, entre otros.

(187) En estos casos, no será aplicable porque "la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por la ley. En tales casos, los Estados miembros establecerán las garantías apropiadas" (art. 11-2, Directiva).

(188) Texto completo en: WWW. UMONTREAL. EDU. CA.

El principio de *"Storage and security of information"*, aplicable a esta fase del procedimiento informatizado estudiado está previsto en la ley especial australiana referenciada que establece, lo siguiente: El responsable (persona natural o jurídica, pública o privada) de la posesión o administración de datos o informaciones (registros desde el punto de vista iusinformático) esta obligada a: a) guardarlos de conformidad con los propósitos o fines explícitos, legales y con los usos determinados para aquéllos; b) almacenar los datos o informaciones en forma adecuada y pertinente, sin exceder los propósitos para los cuales fue almacenado (es decir, que exista proporcionalidad de los fines en la recolección y almacenamiento de los datos); c) confirmar que el procedimiento informático hasta esta etapa se ha realizado en forma justa y legal; d) Almacenar los datos por un lapso de tiempo necesario de conformidad con los fines perseguidos con dicha actividad; e) Proteger los datos almacenados aplicando medidas idóneas de seguridad contra la posible pérdida, acceso desautorizado, modificación, descubrimiento y/o divulgación no autorizados; y en general, contra el uso indebido de los mismos; y f) Suministrar la información concerniente a una persona y en poder del responsable de la misma, siempre que con esta actividad se prevenga un uso desautorizado o un descubrimiento de información no autorizada (Art. 21).

5.2.1.2.2. REGISTRO Y CONSERVACION ELECTROMAGNETICA DE LOS DATOS .

¿Qué se entiende por registro de datos desde el punto de vista iusinformático?, es la gran pregunta que debemos hacernos en éste punto, pues tanto la LORTAD, como las normas comunitarias; y en general, las normas que regulan el tratamiento informatizado de datos de

carácter personal, se refieren todas a la actividad iusadministrativa de "*inscripción en el Registro*" de un fichero o banco de datos personales de índole informatizada, pero en manera alguna al registro iusinformático de los mismos, con la salvedad de la LORTAD, que hace referencia tácita a éste como veremos. En efecto, los cuerpos normativos sobre tratamiento informatizado de datos personales (LORTAD: LO 5/1992, 29 Oct.; Convenio Europeo de 1981; Directiva 95/46/CE; Privacy and data Australiana 1994, etc) hacen referencia a la inscripción en el registro de un fichero o banco de datos informatizados que contiene una cantidad de datos considerados personales por el ordenamiento jurídico vigente, y como tales permitida su recolección y posterior almacenamiento electromagnético. Esta actividad es realizada, por regla general, por un organismo autónomo y colegiado creado al efecto, de régimen jurídico administrativo o *sui géneris* como en el caso español [189] que cumple funciones de registro, vigilancia, control, administración e incluso sancionatorias y correctivas.

El Registro de datos desde el punto iusinformático o *registro informático* [190], abarca no sólo la actividad iusadministrativista de la inscripción informática ante una autoridad competente de un fichero o banco de datos contentivo de información catalogada como personal, sino también la previa e ineludible actividad electromag- nética de la grabación (*save*) y confirmación del *storage electrónico de datos* digitales (texto, sonido o imágenes) en y con soportes y medios informáticos, electrónicos y telemáticos. Es decir, que el registro iusinformático contiene una etapa *a priori* y de carácter interna y otra, *a posteriori* de carácter externa. La primera se verifica por y ante la misma persona natural o jurídica, pública o privada titular del fichero o banco de datos; y la segunda, se lleva a cabo ante la autoridad competente para crear, llevar, gestionar y cumplir los fines y funciones del Registro General de los ficheros o bancos de datos de carácter personal de conformidad con el ordenamiento jurídico vigente.

La distinción de estas dos etapas en el registro de datos interesa determinarla a los siguientes efectos: a) confirmar que los datos de carácter personal son informaciones concernientes a las personas. En particular, toda información alfanumérica, gráfica,

---

(189) La Agencia de Protección de los Datos. "El art. 6.5 LGP quedará en la historia de derecho público como ejemplo de lo arriesgado que resulta el poner en manos de los adoradores del Poder preceptos tipo ´cajón de sastre´. No es el momento de estudiar este precepto. Recuérdese, sin embargo, que dicha ley va agru-pando sucesivamente las distintas organizaciones que integran el sector público en organismos autónomos (de carácter administrativo y de carácter comercial, industrial, financiero y análogos) (art. 4.1), Seguridad social (art. 5), sociedades estatales (con participación estatal mayoritaria y entidades de derecho público) (art. 6.1), y "el resto del sector público" (art. 6.5). Esta última frase ha permitido abrir un portillo por el que una serie de organizaciones a las que se conoce ya en la doctrina con el calificativo de organizaciones independientes (tomado, ciertamente, de la terminología que utiliza la norma de creación correspondiente a cada una de ellas) han empezado a buscar el camino de la ´libertad´(entiéndase: de la reducción al máximo de cualquier forma de control). Ello ha dado lugar a un problema de enorme gravedad sobre el que ya ha dado la voz de alerta por algunos autores (v.gr. Silvia del Saz). GONZALEZ NAVARRO, F y

GONZALEZ PEREZ, J. COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LA ADMINISTRACION PUBLICA Y PROCEDIMIENTO ADMINISTRATIVO COMUN. 1a. ed., Ed. Civitas, S.A., Madrid, 1997, pág. 705.

(190) A los efectos de este trabajo "Registro informático", es aquél derivado del análisis de la terminología utilizada por la LORTAD y las normas comunitarias que regulan el tratamiento informatizado de datos. En efecto, La LORTAD, al definir "tratamiento de datos" hace alusión a las operaciones y procedimien-tos técnicos, de carácter "automatizado" que permitan la "recogida, *grabación*, ..." (Art.3, c,); en tanto que la Directiva 95/46/CE, utiliza el término "registro" para conceptualizar esa misma parte del tratamiento informatizado de datos (art. 2, b), con lo cual registro informático tiene una doble construcción: una parte tecnológica fundada en la grabación de datos o informaciones con soportes y medios informáticos, electrónicos o telemáticos; y una parte, jurídica, la del registro como actividad jurídico-administrativa.

fotográfica, acústica, o de cualquier otro tipo susceptible de ser recolectada, *registrada*, tratada o transferida concerniente a una persona física identificada o identificable, por soportes y medios informáticos; b) Verificar y confirmar que los datos personales son susceptibles de almacenamiento y registro electromagnético. Se descartan los datos no susceptibles de procedimiento informático, es decir, los sujetos a tratamiento no informatizado; y ,c) En el caso de la legislación especial de tratamiento informatizado de datos española (LORTAD), la determinación, el momento y oportunidad jurídico-legal de iniciación del "*procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos*", que regulará por el Ministerio de Justicia, por vía reglamentaria, aún no desarrollado (art. 38-3)

Muy a pesar de ello, se ha dado más relevancia a la actividad a posteriori o externa del registro informático, más que a la previa por considerarla una fase enteramente tecnológica y casi sin incidencia jurídica. El Real Decreto No. 263 de Febrero 16 de 1996, que reguló la utilización de técnicas electrónicas, informáticas y telemáticas, vino a llenar en parte ese vacío legislativo, por lo menos en el ámbito del sector público, en el caso español [**191**]. En una y otra etapas del registro informático se abren y cierran amplios portales de riesgo, vulneración o consolidación de derechos y deberes para los titulares de datos personales, de ficheros o bancos de datos e incluso de terceros que son dignos de estudiarse desde la óptica de los principios de protección y seguridad de los datos. Ciertamente, en el ámbito de la legislación de tratamiento informatizado de datos español, en forma expresa y con base en el principio de seguridad de los datos, se hace referencia a las dos etapas del registro informático cuando se prohíbe el registro de los datos de carácter personal contenidos en ficheros o bancos de datos informatizados que no reúnan las condiciones que se determinen por vía reglamentaria (por el Ministerio de Justicia) con respecto a su integridad y seguridad y a los centros de tratamiento, locales, equipos, sistemas y programas (Art. 9 LORTAD).

Pese a todo, a nivel de la legislación española, se enfatiza en el registro informático en su fase externa, el cual se adelanta ante un órgano integrado en la "Agencia de Protección de datos" (art.38, LORTAD), denominado *Registro General de Protección de Datos*, reglamentado por el Real Decreto No. 428 de Marzo 16 de 1993, al que corresponde velar por la publicidad de la

existencia de los ficheros o banco de datos informatizados de carácter personal, con miras a viabilizar el pleno ejercicio de los

---

(191) Véase, apartados 2.4 y ss., de la parte III de este trabajo.

derechos de información, acceso, rectificación y cancelación de datos previstos en los artículos 13 y 15 de la L.O. 5/1992, de Oct. 29. (Art. 23). Igualmente tiene funciones de instrucción de procedimientos de inscripción en el Registro, instrucción, certificación y publicación periódica de anuarios de ficheros o bancos de datos notificados e inscritos[192].

Son objeto de inscripción en el Registro General de Protección de datos, los siguientes ficheros o bancos de datos, actos y documentos: a) Los que sean titulares las Administraciones Públicas [193]. En los asientos de los ficheros de titularidad pública figurará, la información contenida en la disposición general de creación o modificación del fichero, de conformidad con el art. 18.2., LORTAD [194] (Art. 24-2. R.D.428 de Marzo 16 de 1993), b) Los de titularidad privada. En los asientos de inscripción de estos ficheros figurarán la información contenida en la notificación del fichero a excepción de las medidas de seguridad, así como los cambios de finalidad del fichero (Art. 24-3, R.D.428 de Marzo 16 de 1993). c) las autorizaciones en materia informática, tales como las autorizaciones de transferencia temporal o definitiva de datos personales a otros países, siempre que medie autorización del Director de la Agencia de Protección de Datos, y los países ofrezcan un nivel de protección equiparable al de España, sobre

---

(192) Cfr. Inscripción y certificaciones.1. Corresponde al Registro General de Protección de Datos instruir los expedientes de inscripción de los ficheros automatizados de titularidad privada y pública. 2. Corresponde asimismo al Registro General de Protección de Datos: a) Instruir los expedientes de modificación y cancelación del contenido de los asientos. b) Instruir los expedientes de autorización de las transferencias internacionales de datos.c) Rectificar de oficio los errores materiales de los asientos. d) Expedir certificaciones de los asientos. e) Publicar una relación anual de los ficheros notificados e inscritos (Art. 26. R.D. Núm. 428/1993, Marzo 26. R.D). en: AA.VV. *DISCOS COMPACTOS ARANZADI*. Ed. Aranzadi, S.A. Madrid, 1998

(193) Cfr. *Ficheros de las Administraciones Públicas*. Serán objeto de inscripción en el Registro los ficheros automatizados que contengan datos personales y de los cuales sean titulares: a) La Administración General del Estado, b) Las entidades y organismos de la Seguridad Social, c) Los organismos autónomos del Esta- do, cualquiera que sea su clasificación, d) Las sociedades estatales y entes del sector público a que se refiere el artículo 6 de la Ley General Presupuestaria, e) Las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros a que se refiere el artículo 40.2 de la Ley Orgánica 5/1992, f) Las entidades que integran la Administración Local y los entes y organismos dependientes de la misma (Art. 24-1. R.D. Núm. 428/1993, Marzo 26). Texto completo en: AA.VV. *DISCOS COMPACTOS ARANZADI. Ed. Aranzadi, 1998.*

(194) *Cfr. Los ficheros de titularidad pública*. Art. 18-2. Las disposiciones de creación o de modificación de los ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo, b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos, c) El procedimiento de recogida de los datos de carácter personal, d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo, e) Las cesiones de datos de carácter personal que, en su caso, se prevean, f) Los órganos de la Administración responsables del fichero automatizado, y, g) Los servicios o unidades ante los que pudiesen ejercitarse los

derechos de acceso, rectificación y cancelación. Texto completo en: AA.VV. *DISCOS COMPACTOS ARANZADI. Ed. Aranzadi, 1998.*

tratamiento informatizado de datos (Art.25, (a), R.D.428 de Marzo 16 de 1993; conc. Art. 32, LORTAD), d) *Los códigos tipo*, que con el carácter de normas deontológicas o de buena práctica profesional, se formulan por los responsables de los ficheros de titularidad privada. (Art.25, (b), R.D.428 de Marzo 16 de 1993; conc. Art. 31, LORTAD [195], d) los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación (Art. 24-4 R.D.428/93 de Mar.16; conc, Arts.13 -15 y 38-3, LORTAD).

En consecuencia, no son objeto de inscripción en el Registro, y por tanto, sujetos de las medidas de protección y seguridad referida a los datos de carácter personal según el ordenamiento jurídico, los datos excluidos de la relación *numerus clausus* anterior. Sin embargo, cabe interpretar también que no son objeto de inscripción, los ficheros o bancos de datos, cuya información o datos se halla prohibida someterla a procedimiento o alguna fase del tratamiento informatizado según el ordenamiento jurídico. En efecto, quedarían por fuera de la inscripción todos los ficheros que según la LORTAD, se excluye del tratamiento informatizado en forma taxativa, a saber: a) Los ficheros de titularidad pública, cuyo objeto sea el almacenamiento de datos para su publicidad con carácter general, b) los ficheros mantenidos por personas físicas con fines exclusivamente personales, c) los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales, d) 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) 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 LORTAD, salvo que resultara de aplicación el artículo 7 LORTAD, por tratarse de los datos personales

---

(195) Cfr. *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 equi-pos, 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. 31, LORTAD). Texto completo en: AA.VV. *DISCOS COMPACTOS.... Ed. Aranzadi, 1998.*

en él contenidos. Esta exclusión del tratamiento y de la consiguiente inscripción en el Registro queda explicada en la E. de M. de la LORTAD, al precisar por "exclusión" el ámbito de aplicación de la misma [196] .

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* [197], al referirse al principio 5 del art. 21 *ab initio*, sobre la "information relating to records kept by record-keeper", proporciona una serie de directrices aplicables a la fase de registro informático y las subsiguientes actividades de la persona concernida con una información personal, los responsables de un fichero o banco de datos y los derechos y deberes derivados del almacenamiento y registro de datos para unos u otros.

Estas son: 1.El responsable de la posesión o administración de ficheros o bancos de datos que contienen información personal registrada, tomará las medidas necesarias y legales para permitirle a cualquier persona determinar, lo siguiente: a) Si el responsable de la posesión o administración de los ficheros o banco de datos, tiene en sus archivos información personal, b) Si esa información personal registrada le concierne a una determinada o determinable persona, c) Si el responsable de la posesión y administración de los ficheros o banco de datos contiene información personal, con la cual: i) se repute de su naturaleza, ii) se determine los propósitos principales para los cuales se utiliza la información; y, iii) se pueda acceder a la información personal registrada. 2. El responsable de los ficheros o banco de datos que no haya sido registrada bajo los pasos del numeral anterior, podrá negarse a dar acceso a la información contenida en éstos, de conformidad con las leyes estatales especiales que rigen en la materia para los documentos.

Ahora bien, una vez se ha registrado los datos o informaciones de carácter personal, conforme al ordenamiento jurídico vigente por las autoridades competentes se

---

(196) En efecto, "a título de ejemplo (se) relaciona los datos de carácter personal y los ficheros o banco de datos que los contienen que no son objeto de la LORTAD, y por tanto, no son inscribibles en el Registro mencionado. Sostiene, quedan por fuera "los datos anónimos, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general --como pueden ser los registros de la propiedad o mercantiles--, así como, por último, los de uso estrictamente personal. De otro lado, parece conveniente la permanencia de las regulaciones especiales que contienen ya suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico. Así ocurre, por ejemplo, con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así acontece, también, con los ficheros regulados por la Ley 12/1989, de 9 de mayo (RCL 1989\1051 y RCL 1990\1573), sobre función estadística pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. En fin, quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses público prevalentes, no deben estar sometidos a su régimen cautelar". Texto completo en: AA.VV. *DISCOS ARANZADI. Ed. , 1998.*

(197) Texto completo en: WWW.UMONTREAL. EDU.CA.

produce una subfase que va ligada al registro, aunque puede identificarse desde el punto de vista jurídico e incluso técnico. Jurídicamente conservar un dato o información personal significa mantenerla en las condiciones de forma y tiempo, fines, propósitos y naturaleza para las cuales fue recolectada, almacenada y registrada por las personas naturales o jurídicas, públicas o

privadas, según el ordenamiento jurídico vigente. Tecnológicamente, conservar un dato o información personal es mantener en y con medios electromagnéticos en condiciones de forma y tiempo óptimas que permitan *en o a prosteriori* el acceso, uso, utilización y transferencia legítimas por quienes están autorizados por la ley o mandato judicial para esto.

El Convenio de Estrasburgo de 1981, al hacer referencia a un grupo de principios que deben observar los datos de carácter personal que sean objeto de un tratamiento automatizado, bajo el epígrafe de "calidad de los datos"; entre otros, principios, expone el principio y a la vez característica de los datos sometidos a procedimientos informáticos, cual es la conservación de los mismos tanto jurídica como técnicamente. En efecto, expresa que "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),) .

En el ámbito ibérico, la conservación de la información o datos, desde el punto de vista tecnológico, por lo menos en el sector público, esta guiada por las directrices expuestas en el R.D. Núm. 263 de 1996, Febrero 16, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. En lo pertinente sostiene: Cuando se utilicen los soportes, medios y aplicaciones referidos en el apartado anterior, *se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.* Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos. Las medidas de seguridad aplicadas a los soportes, medios y aplicaciones utilizados por los órganos de la Administración General del Estado y sus entidades de derecho público vinculadas o dependientes deberán garantizar: a) La restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas. b) La prevención de alteraciones o pérdidas de los datos e informaciones (Art. 4-2 y 4-3).

Jurídicamente, en el derecho español, la conservación de los datos personales sujetos a procedimiento informatizado, está prevista en varias normas de la LORTAD, pero por sobre todo, bajo la calidad y forma de principios que rigen la protección y seguridad de los datos personales.

En la E. de M., de la LORTAD, se plasma como columna vertebral:

> *Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos*

subjetivos ahora aludidos, no rebasarían un contenido meramente programático (considerando 3).

Souviron [198], ubica dentro de la calidad y veracidad de los datos, el almacenamiento y conservación de los datos personales. Al referirse a éste último, expresa que los datos "deberán ser conservados durante los plazos previstos en las disposiciones aplicables, o en caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado (art. 15.5 LORTAD), y ello en los términos ya expuestos respecto a su conservación y cancelación, serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado. Consecuentemente, si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos por los correspondientes datos rectificados o completados de oficio o a instancia de los afectados (Art.4.3. y 4 y 15)", [Leáse titular de los datos en lugar de "afectado", por las suficientes razones anteriormente suministradas al efecto].

La conservación de los datos personales en el marco de la LORTAD, además de principio característico de los procedimientos informatizados, constituye un tipo de infracción de carácter "leve", cuando es inobservado por los responsables de los ficheros. En tal virtud, "no conservar actualizados los datos de carácter personal que se mantengan en ficheros" informatizados, constituye una infracción leve investigada y sancionada por las autoridades competentes de protección y seguridad de los datos personales en el derecho español (Art. 43, (c), y 45).

En la Directiva 95/46/CE, siguiendo los pasos del Convenio Europeo de 1981 y la LORTAD, bajo el epígrafe de los "principios relativos a la calidad de los datos", expresa que los Estados miembros dispondrán que los datos personales sean: "conservados 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

---

(198) SOUVIRON, J.M. *EN TORNO A LA JURISDICCION DEL PODER*...Ob. cit., pág. 152

fines históricos, estadísticos o científicos" (Art. 6, (e),).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* [199], al referirse al principio 5 del art. 21 *in fine*, sobre la *information relating to records kept by record-keeper*, hace mención a la conservación de los datos personales registrados, al sostener: 3. El responsable de un fichero o banco de datos personales registrado deberá conservarlo: a) porque la naturaleza de información personal así lo requiere; b) porque constituyen fuentes de información personal, c) porque contiene unos propósitos definidos desde la recolección de la misma por la autoridad

correspondiente, d) porque cada información guarda relación con los propósitos generales del fichero, e) porque se individualiza la información personal guardada, f) porque se determina el período para cada tipo de información registrada, g) porque se identifica plenamente a las personas titulares del derecho de acceso a la información contenida en los ficheros, así como las circunstancias o requisitos exigidos para éste; y, h) porque determina los trámites o secuencias seguidas para ejercer el derecho de acceso a la información personal. 4. El Responsable de un fichero o banco de datos, esta obligado: a) mantener esta información personal registrada, según el numeral anterior, disponible para la inspección de las autoridades competentes, y b) Informar en el mes de junio de cada año, al Comisionado para la protección a la intimidad, así como enviar una copia del registro de la información personal que las autoridades competentes están autorizadas a conservarla.

5.2.1.3. FASE DE SALIDA DE DATOS O FASE *OUTPUT*

Toda fase de salida de datos de cualquier sistema en los que se emplea, aplica, desarrolla y concluye las tecnologías TIC y metodologías de la informática , se conoce como *fase output de datos o informaciones*. Esta fase del procedimiento informatizado realizado en un sistema de tratamiento de datos o informaciones con relevancia en el ámbito del derecho, con soportes y medios informáticos, electrónicos o telemáticos, se verifica de diferentes formas y para predeterminadas finalidades establecidas en el ordenamiento jurídico. Como lo sostiene el iusinformático *López Muñiz-Goni* [200], tales sistemas de tratamiento informatizado de datos, en su fase de salida, son: a) el sistema referencia, b) el sistema de resúmenes o de *abstract*, y c) el sistema de texto completo o *full text*.

Estos sistemas de tratamiento informatizado de la información, en cuanto a su

---

(199) Texto completo en: WWW.UMONTREAL.EDU.CA.

(200) LOPEZ MUÑIZ-GONI, M. Ob ut supra cit., pág. 39-40. Veáse nota de pie de página núm. 162, en cual se hace mención a los sistemas de tratamiento informatizado relacionados para el momento informático del *input* de datos.

descripción teórica basada en descriptores (o palabras claves ordenadas lógicamente en un thesauro) o en resúmenes o texto completo de una serie de documentos, datos o informaciones previamente tratadas con soportes y medios informáticos con similares técnicas y metodologías propias de la lógica informática en la fase *input* de datos (recolección, selección y organización), se despliegan para la fase *output* de datos, con la obvia aclaración de que la información o datos de cualquier tipo en ésta última fase tienen por objeto la extracción, recuperación o transferencia para la simple consulta, traslado, cesión o intercambio de datos, a través de vías *off line* (fuera de sistemas de redes de información) u *on line* (vías de red de redes de información: locales o intranet´s o globales o prototípicas de internet´s) respectivamente, por el titular de los datos, los responsables de los ficheros o banco de datos o las personas naturales, jurídicas, públicas o privadas, autorizadas por el ordenamiento jurídico o autoridad competente para hacerlo.

Por lo anterior, podemos distinguir desde el punto de vista tecnológico con incidencia en el ámbito jurídico en esta fase *output* de datos, distintos mecanismos de output de información, dependiendo de si los datos extractados, recuperados o transferidos en un sistema informático, con medios informáticos, electrónicos o telemáticos, destinados para prestar servicios fuera de los sistemas de red de redes de información o sistemas *off line;* o por el contrario, se hacen dentro de un sistema infor-
mático conectado a un sistema de red de redes de información o sistema *on line*; o más aún, si se hace en un sistema que une las características, finalidades y funciones generales y especiales de uno y otro sistema. Estos últimos sistemas que son los que hoy en día se utilizan en todas las actividades que emplean soportes y medios informáticos, electrónicos y telemáticos, podríamos llamarlos sistemas *duplex (off and on line).*

Básicamente los dispositivos, equipos o sistemas informáticos de finales del siglo XX, tienen una estructura, finalidades y funcionamiento de los dos sistemas (off y on line), aunque antes de masificarse las nuevas tecnologías de la información o comunicación (TIC), los equipos computacionales prestaban servicios electrónicos de ingreso, selección, organización y recuperación para consulta de la información, pero no los de transferencia o traslado de datos entre equipos o sistemas computacionales, así estuviesen ubicados en una red local (intranet´s), o más aún, en una red global (internet´s) por más sofisticados que estos equipos fueran. Sólo a partir del avance de las tecnologías TIC y como también lo sostiene el profesor *Ethain* [201], con la popularización, la interconexión de computadores vía MODEM a una red de redes de información, el manejo digital de la misma (ya sea texto, imagen o sonido) y las ventajas

---

(201) Ethain, K. *RIGHTS, CAMERA AND ACTION*... En: WWW.UMONTREAL. EDU. CA.

electrónicas de la utilización del hipertexto, se viene ha estructurar una cultura electrónica que permite, entre otras funciones principales, las básicas de todo dispositivo, equipo o sistema computacional y la transferencia de datos en un sistema *duplex.*

A los efectos de este trabajo y desde el punto de vista la normativa comunitaria, española y australiana sobre tratamiento informatizado de datos de carácter personal, los sistemas de tratamiento de datos en el ámbito del derecho, como mecanismos tecnológicos utilizados para la extracción, recuperación y transferencia de datos, se pueden distinguir entre los sistemas de tipo general y los sistemas de carácter especial. Los primeros, hacen referencia a todos aquellos procedimientos informatizados que tienen por objeto la recuperación, intercambio o trasmisión de datos personales generales [202], de los datos personales denominados “sensibles” (cuando se permita por la legislación de los Estados, por excepción) [203]; así como de los datos

personales accesibles al público contenidos en ficheros públicos o privados (en los cuales prima el interés de colectividad sobre el del concernido, según *Van der Mensbrugghe* [204]), a

---

(202) Según la clasificación de J.M., Souvirón que distingue entre "datos personales de carácter general" y datos de carácter personal o "sensibles". Los primeros, son aquellos correspondientes a " cualquier información concerniente a personas físicas identificadas o identificables"; y los segundos, aquellos datos personales "relativos a la ideología, religión o creencias y los que hagan referencia al origen racial, a la salud y a la vida sexual". Estos últimos en la legislación sobre tratamiento informatizado de los datos personales en España, "son objeto de protección reforzada sobre la base del principio del consentimiento del afectado". Vid. SOUVIRON, J.M. *EN TORNO A LA JURIDIFICACION DEL PODER...* Ob. ut supra cit., pág. 162-163.

(203) Véase, la parte IV, punto 5.2.3. y ss., en los cuales abordamos el tema de los datos "sensibles", " hipersensibles " y los diferentes niveles de protección y garantía estatal dado en la LORTAD y las normas comunitarias.

(204) *Datos accesibles al público***:** los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos y análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de pertenencia al grupo. Vid. COLECCION DE DISCOS ARANZADI. Aranzadi S.A., 1998. Para DE VAN DER, Patricia. "Que los ficheros estatales o privados estén al libre acceso del público en general presenta para el ciudadano varios riesgos: de una parte el hecho que la persona quiera guardar la confidencialidad de ciertos datos (estados de salud, infracciones penales, períodos de inestabilidad laboral, etc.). De otra parte, el hecho que el ciudadano viva bajo la incertidumbre y en la inseguridad de no saber de qué manera se utiliza la información que conciernen a su espacio de vida privada por la utilización de datos falsos o inexactos. Es sobre toda la injerencia en la vida íntima, el no respecto a ese espacio de autonomía que le corresponde como ente individual. Pero ese espacio de "intimidad", "de privacidad individual", se limita en la medida que la sociedad en general requiere del individuo ciertas informaciones. El derecho a la información que tiene la colectividad sobre los datos del particular aparece así en contrapartida. Entonces resulta lógico pensar que en los servicios de policía o penitenciarios se pidan datos de si ha habido condenas anteriores, o que en servicios de salud se conozcan las enfermedades que han sido contraídas anteriormente, o que un patrón solicite la información de los antiguos lugares de trabajo." Cfr. VAN DER MENSBRUGGHE, Patricia. FLUJOS TRANSFRONTERIZOS DE DATOS EN LA DIRECTIVA 95/46 DE LAS COMUNIDADES EUROPEAS. En: Revista Actualidad informática Aranzadi. No. 20 Julio, Elcano (Nav.), Madrid, 1996, pág.3.

través de soportes y medios informáticos, electrónicos o telemáticos en sus respectivos territorios y con los objetivos y finalidades previstos en los ordenamientos jurídicos vigentes. Los segundos, hacer referencia a todos los procedimientos informatizados que con similares técnicas, metodologías, objetivos y fines perseguidos para los primeros, se realizan para la recuperación, intercambio o trasmisión de datos personales, entre diferentes Estados en un régimen transfronterizo, internacional dentro de los que quedan incluidos los regímenes denominados "a terceros países".

5.2.1.3.1. LA FASE OUTPUT GENERAL DE DATOS.

La última fase del procesamiento informatizado de datos de carácter personal, empleando sistemas de tratamiento de salida (/S) de la información (de referencia, de resúmenes o de texto completo: Thesauro y descriptores), es también conocida como de output de datos, siempre que se utilice soportes y medios informáticos, electrónicos o telemáticos (de software y de hardware

[**205**]), tengan objetivos previstos en el ordenamiento jurídico y persigan las finalidades de recuperación, intercambio o trasmisión de datos en los mismos Estados donde se produjo en su totalidad las fases previas del ciclo informático y que antes hemos visto y analizado.

En esta fase de salida de datos, es importante estudiar el tríptico fundamental de derechos que estructuran el derecho de *habeas data*, es decir, el derecho de acceso, rectificación o actualización y el de cancelación de la información, por cuanto cada uno de ellos desde el punto de vista jurídico, más que tecnológico inciden en el dual mundo de la paradoja, estructurado por un lado, por la protección y garantía de los derechos y libertades públicas por parte del Estado o las personas naturales o jurídicas, públicas o privadas que deben hacerlo; y de otro lado, en el variopinto espectro del desconocimiento, la vulneración, el quebrantamiento o la negación de esos derechos, libertades públicas e intereses legítimos.

5.2.1.3.1.1. EL HABEAS DATA EN LA FASE DE OUTPUT GENERAL DE DATOS EN LA LEGISLACION ESPAÑOLA.

Hemos dicho que la Agencia de Protección de Datos en España, es una

---

(205) Véase, Parte III, punto 2.4.1, 2.4.2.; 4, 4.3.1. y 4.3.2. Así mismo la parte IV, de este trabajo referida a la denominada "parte *in fine* del tipo: La interceptación o intervención" (punto 5.2.2.2.), en los cuales nos referimos a la trasmisión electrónica de la información ("Comunicación electrónica de datos", en especial, los de carácter personal).

institución *sui géneris* con régimen jurídico administrativo de carácter independiente de las Administraciones Públicas, personalidad jurídica propia y plena capacidad pública y privada, cuya función principal es velar por el cumplimiento de la legislación sobre protección de datos personales informatizados y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

El derecho a la información que tiene cualquier persona en el procedimiento informatizado se manifiesta en las diferentes etapas del mismo, tal y como se desprende de los arts. 5 y 12 de la LORTAD, pues no sólo la persona tiene y debe estar informada en el momento de la recolección de los datos personales que le conciernen y de los derechos subsecuentes de acceso, rectificación o actualización y cancelación, según fuere el caso, sino durante las etapas del procedimiento informatizado subsiguientes; sobre todo, una vez que se hallan almacenados por parte de las personas naturales o jurídicas, públicas o privadas respectivas, según el ordenamiento jurídico vigente y registrados y aplicadas las medidas necesarias de seguridad y conservación de datos por las correspondientes autoridades competentes de la inscripción en el registro, control, administración y gestión de los mismos como la Agencia de Protección de Datos (y en su nombre el Registro General de Protección de datos).

Ante el Registro se puede consultar la finalidad, estructura, identidad del responsable del fichero, ubicación, cesiones previstas, etc., pero no los datos *strictu sensu* contenidos en los ficheros respectivos, pues como se comprende éstos sólo los poseen los responsables del fichero y ante quienes se ejercita los derechos de acceso, rectificación y cancelación. El responsable del fichero, con base en dicho ejercicio podrá si así se desprende del ejercicio de estos derechos, rectificar o cancelarlos, o conferir el acceso al titular de los datos sobre aquéllos. Si los responsables de los ficheros desatienden las solicitudes del titular de los datos, la LORTAD, ha previsto en vía administrativa el Procedimiento de Tutela de Derechos (art. 17 de la LORTAD y art. 17 del RD. 1332/94), o en vía contencioso-administrativa, sobre las resoluciones del Director de la Agencia de Protección de Datos (art. 17-2 LORTAD).

El derecho de acceso a los datos o informaciones personales, según *Orti Vallejo*[206], consiste en la facultad del afectado (por titular de los datos) de conocer si un fichero contiene datos personales suyos y el contenido de los mismos, para, en su caso, instar la rectificación o cancelación, ante los responsables de los ficheros correspondientes. Aunque el autor citado duda que la LORTAD, no sostiene expresa -

---

(206) ORTI VALLEJO, A. *DERECHO A LA INTIMIDAD*... Ob. cit., págs. 162-163

mente en el art. 14, que deba ejercitarse el derecho de acceso ante el responsable del fichero, pero sí los subsecuentes derechos de rectificación, actualización o cancelación, los cuales tienen expresa mención en los arts. 15 y 16 (reglamentados por los artículos 12 y 13 del Real Decreto 1332/94); es apenas obvio según el aforismo latino que *lo accesorio sigue la suerte de lo principal* (tomándolo con tal, a los solos efectos de probar este simil, el derecho de información), y aquí lo principal es el derecho de acceso a la información a efectos de recuperar información con fines de mera consulta, intercambio o transferencia de datos, según fuere el caso y circunstancias previstas en el ordenamiento jurídico o por orden de autoridad competente (art. 14-2).

El derecho de acceso sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el titular de los datos acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes (art. 14-3). Se entiende que el término previsto en la LORTAD, sólo puede empezarse a contar una vez el fichero se halle registrado conforme al procedimiento y trámites anteriormente, pues de lo contrario es inocuo cualquier término. Igualmente el término, constituye "una garantía complementaria para la persona concernida", según el Convenio Europeo de Protección de datos de carácter personal, de Estrasburgo, de 18 de Enero de 1981, para conocer "la confirmación de la existencia o no" de datos pertenecientes a una persona, así como la "comunicación de dichos datos en forma inteligible" (art. 8, (b),) y como un derecho

"del ciudadano contra abusos de los *almacenistas* (utilizado por el autor con cierta crítica ácida) de datos personales, sean privados o públicos", según *Fairen Guillén* [207].

He ahí, porque sostenemos que el derecho a la información previo al ejercicio del derecho de acceso está presente en todo el ciclo informatizado de un sistema de datos, máxime cuando se trata de datos catalogadas de personales. Sin embargo, asalta una duda razonable sobre los términos utilizados para el ejercicio y concesión del derecho de acceso a los datos contenidos en ficheros informatizados, en una forma y términos diferentes a los tradicionales (dentro de la lógica del mundo escriturario o del impreso) y no dentro de la lógica electrónica de *Ethain*, que tiene como característica la ruptura del concepto tradicional de formatos y tiempo. El solicitante de una información o datos por soportes o medios informáticos, lo podrá hacer desde su casa, oficina, lugar de trabajo, etc., sin necesidad de ir físicamente ante un despacho u oficina, siempre que cuente con un equipo de software y hardware idóneos, la base de datos o ficheros esté disponible y tenga una especie de "alta" para el ingreso a la misma, previos la identificación general (nombres, apellidos, etc) y electrónica (con una clave de acceso alfanumérica) o *password* y que el fichero este *on line*, o mejor aún, en sistema *duplex*.

Pese a ello, las condiciones actuales del solicitante de datos que le conciernen son diferentes en la fase output o de salidad de datos, aún cuando éstos han seguido un procedimiento con tratamiento informatizado (con soportes y medios electromagnéticos) desde la recogida, hasta el almacenamiento y el registro del fichero por y ante las personas naturales, jurídicas, públicas o privadas, encargadas de hacerlo. En efecto, el ejercicio del derecho de acceso a los datos (tecnológicamente ingreso o *enter*), con finalidades de mera consulta, o más aún transferencia de datos, etc., todavía sigue haciéndose dentro de la lógica tradicional en forma, tiempo y circunstancias (formularios petitorios, términos para la solicitud, decisión, concesión, etc: todo dentro de la lógica de la cultura del impreso o la escritura).

En tal virtud, conviene que la normativa que reglamenta el tratamiento informatizado de los datos de todo tipo; y en forma especial, los de índole o carácter de personales, se atempere plenamente a la forma, tiempo y circunstancias del fenómeno que esta regulando, en todas las fases del ciclo informático; y sobre todo en la fase de salida de datos (acceso, rectificación, cancelación y actualización).

En todo caso, hoy por hoy, el procedimiento administrativo para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente, según la ley (art. 16-1 LORTAD). Sin embargo, la E. de M., y la propia LORTAD en su articulado establecen las directrices para dicha reglamentación. Hemos dicho que se hace por solicitud o petición dirigida al responsable del fichero, a través de soportes y medios informáticos,

electrónicos o telemáticos que garanticen la identificación del titular de los datos y en la que conste el fichero o ficheros a consultar. El responsable resolverá la petición en el lapso de tiempo prudencial establecido en la ley. Pese a ello, éste podrá denegar el acceso de la información, ya se trate de un fichero público o privado, si en éste último caso la solicitud se ha realizado por persona distinta al titular de los mismos (art.14-1).

En los ficheros de titularidad pública, se podrán denegar, siempre que se trate de los "Ficheros de las Fuerzas y Cuerpos de Seguridad" y los Ficheros de "La Hacienda Pública", que serán regulados como excepciones *numerus clausus* en el sistema de denegación al ejercicio del derecho de acceso por vía legislativa que ha dado lugar a recursos de inconstitucionalidad, aun irresolutos ante el Tribunal Constitucional de España [208]. La E.de M. LORTAD, al respecto sostiene:

> *En concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley. El primero de ellos ha cobrado en nuestro país, incluso, plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones Públicas (artículo 105.b). En consonancia con ello queda recogido en la Ley en términos rotundos, no previéndose más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de este carácter, excepciones ambas que pueden entenderse expresamente recogidas en el propio precepto constitucional antes citado, así como en el Convenio Europeo para la protección de los Derechos Fundamentales.*

---

(207) Vid. FAIREN GUILLEN, A. *EL HABEAS DATA*... Ob.cit, pág. 533.

(208) Los recursos de inconstitucionalidad de la LORTAD, sobre estos puntos en particular planteados por el Partido Popular Español (PP) y demás organismos. Véase, aparte *in fine* de la Parte I.

En efecto, las excepciones son las siguientes:

a) En los casos de los ficheros de las "Fuerzas y Cuerpos de Seguridad" "*para fines policiales"*, (de cuales se excluyen los ficheros creados con igual índole, pero con "fines administrativos"[209]) que contengan datos de carácter personal, cuando su ejercicio pudiera ser una amenaza contra: la defensa del Estado, la Seguridad Pública, la protección de derechos y libertades de terceros, las necesidades de las investigaciones que se estén realizando por parte de los Cuerpos y Fuerzas de Seguridad (art. 20).

b) . En el caso de los ficheros de la "Hacienda Pública" podrá denegarse cuando se obstaculicen actuaciones administrativas tendentes a asegurar el cumplimiento de las

obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras (art. 20 y 21 LORTAD).

---

(209) "Si los datos, por haber sido recogidos ´*para fines administrativos*´ han de ser ´objeto de registro permanente´ tales ficheros estarán sujetos al régimen general de la LORTAD (art. 20-1), obviamente con las particularidades previstas con carácter general para los ficheros automatizados de las Administraciones Públicas. Pero si se trata de datos recogidos ´para fines policiales´ --concepto este que se presume, por oposición al supuesto anterior, que los datos no van a ser objeto de registro permanente-- la cuestión cambia, siendo objeto de un régimen ´ad hoc´... No hay duda de que el régimen de estos ficheros de datos "para fines policiales" es en principio cuestionable. Primero, por lo artificioso que puede resultar la distinción entre tales ficheros (regulados por los apartados 2, 3 y 4 del art. 20, LORTAD) y los que las mismas fuerzas y Cuerpos de Seguridad mantengan ´para fines administrativos´ (regulados por el apartado 1 del mismo artículo), tanto conceptual como operativamente, siendo dudoso que los primeros no constituyan también en la práctica, aunque originados para investigacones concretas y de carácter preventivo, ficheros policiales permanentes (y por ello el art. 20-2 establece que los datos en ese caso ´deben ser almacenados en ficheros específicos establecidos al efecto que deberán clasificarse por categorías en función de su fiabilidad´, es decir, típicos ficheros policiales preventivos no sujetos consecuentemente al principio de veracidad sino --todo lo más-- al de ´fiabilidad´). Segundo, porque tales previsiones están llenas de conceptos jurídicos indeterminados (´fines policiales´, ´prevención de un peligro real´, etc). Y en fin, porque en todo caso resulta muy cuestionable esa no vinculación de las fuerzas y cuerpos de seguridad para recabar y tratar los datos personales, que incluso alcanza a los datos ´sensibles´, sin ningún tipo de intervención judicial u otro organismo de control. Vid. SOUVIRON, J.M. *EN TORNO A LA JURIDIFICACION DEL PODER*... Ob. ut supra cit., pág. 164-165.

c). En el caso de las "Administraciones Públicas", en general, podrá denegarse cuando concurran algunas de las circunstancias siguientes:: a) Razones de interés general (como la Defensa Nacional, la Seguridad Pública o a la persecución de infracciones penales o administrativas), y b) Intereses de terceros más dignos de protección (art.22 Ibídem). Estos intereses públicos prevalentes o intereses de terce- ros más dignos de protección constarán en una "Resolución Motivada" por parte del responsable del fichero. La decisión denegatoria del derecho de acceso a los datos contenidos en el fichero respectivo, podrán ser puestos en conocimiento del Director de la Agencia de Protección de Datos, el cual podrá infirmar o confirmar, según el caso, la procedencia o improcedencia de tal decisión (art. 21 *in fine*).

De otro lado, el garantísmo del derecho de acceso a los datos personales contenidos en ficheros o bancos de datos regulados por la LORTAD, se extiende al ámbito de "protección represiva" de carácter estrictamente administrativo, como lo sostiene el profesor *González Navarro* **[210]**, cuando instituye como *infracciones graves y muy graves*, las que pudiere cometer el responsable de un fichero, encargado o administradores de los mismos, públicos o privados, y consistan en el impedimento o la obstaculización del ejercicio del derecho de acceso y la negativa a facilitar la información que sea solicitada (art. 43.3 (e),) y no cesar en el uso ilegítimo de los tratamientos automatizados de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de datos o por las personas titulares del derecho de acceso (art. 43.4 (d),); respectivamente.

Los derechos de rectificación, actualización y cancelación (tecnológicamente constituyen acciones de modificación y puesta al día [*update*], borrado, eliminación o supresión [*erase o delete*] de datos), previstos en el art.15 de la LORTAD, constituyen derechos determinables e identificables por separado, pero que siendo derechos subsecuentes del derecho al acceso de la información o los datos contenidos en un fichero o banco de datos, constituyen una especie de derechos en cascada e innegablemente complementarios y de efectos jurídicos recíprocos. En efecto, el derecho a la rectificación que tiene toda persona titular de los datos personales que le conciernen, consiste en la facultad o capacidad que aquél tiene para solicitar al responsable del fichero, a fin de que mantenga la exactitud de los datos, rectificando o cancelando los datos personales que resulten incompletos, inexactos, inadecuados o excesivos, según fuere el caso. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación y cancelación efectuada al cesionario. No obstante, cuando se trate de datos que reflejen hechos constatados en un

---

(210) GONZALEZ NAVARRO, Francisco. *COMENTARIOS A LA LEY*... Ob. cit., pág. 711

procedimiento administrativo, aquéllos se considerarán exactos siempre que coincidan con éste (art. 15 de la LORTAD y art. 15 del R.D.1332/1994). El derecho a la actualización de los datos es el resultante del ejercicio de rectificación y cancelación, pues sea por que los datos no tienen las características para ser mantenidos con exactitud, sea por que tras comprobar que no era exactos, se procedió a cancelarlos, los efectos jurídicos y materiales del ejercicio y cumplimiento de esas dos facultades por el responsable del fichero, dará como resultado la actualización o puesta al día de los datos personales resultantes.

Estos derechos de rectificación y cancelación y el resultante de actualización se ejercerá por el titular de los datos, plenamente identificado ante el responsable del fichero**.** La rectificación se hará efectiva por el responsable del fichero dentro de los cinco (5) días siguientes al de la recepción de la solicitud: a) Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario en el plazo de cinco días, b) Si el titular considera que no procede acceder a lo solicitado se lo comunicará motivadamente en el plazo de cinco días, c) Si transcurrido el plazo de cinco días no contesta, podrá entenderse su petición desestimada (art. 15 del R.D. 1332/94).

El derecho de rectificación y cancelación, tanto de los datos personales contenidos en ficheros privados como de los públicos, podrá ser denegado por el responsable del fichero, en las mismas condiciones, circunstancias y excepciones previstas para el ejercicio del derecho de acceso a los mismos datos (art. 15.5 , 21 y 22 de la LORTAD), pues lo accesorio sigue la suerte de lo principal (derecho de acceso a la información).

En cuanto a la "protección represiva" de carácter administrativo de los derechos de rectificación y cancelación de los datos, así como el resultante derecho de actualización de los mismos, la LORTAD, establece como *infracciones leves*, las siguientes: a) no proceder, de oficio o a solicitud de las personas o instituciones legalmente habilitadas para ello, a la rectificación o cancelación de los errores, lagunas o inexactitudes de carácter formal de los ficheros (art. 43.2 (a),); y b) no conservar actualizados los datos de carácter personal que se mantengan en ficheros informatizados (art. 43. 2 (c),). Como *infracciones graves*: a) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente proceden cuando resulten afectados los derechos de las personas que la LORTAD ampara (art. 43. 3 (f),); y b) tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales (v.gr. Habeas data, intimidad, información, etc) (art. 43.4 (f),)

5.2.1.3.1.2. EL HABEAS DATA EN LA FASE DE OUTPUT GENERAL DE DATOS EN LA LEGISLACION COMUNITARIA.

El Convenio Europeo de 1981, al conceptualizar el tratamiento informatizado de datos, los ficheros "automatizados" y los "datos de carácter personal", subsume las etapas del ciclo informático, muy a pesar de que no las exponga en la forma que venimos haciéndolo. Esto no obsta para interpretar que el espíritu de la normatividad especial sobre tratamiento de datos personales sea otra distinta que en la salida de datos o fase output tendrán como fundamento los principios, derechos y obligaciones que rigen tanto para la fase de recolección, almacenamiento e inscripción en el registro los correspondientes ficheros ante las autoridades competentes (o "autoridades controladoras", como lo expresa el Convenio).

En efecto, los principios que guían el tratamiento informatizado de datos personales, como el de **"**Seguridad de los datos" (art. 7), confirman la inclusión dentro del espectro protector la fase output de datos al decir que el principio de seguridad de los datos consiste en tomar las medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra *el acceso*, la modificación o la difusión no autorizados. Así mismo, al establecer las llamadas "Garantías complementarias para la persona concernida", sostiene que una de éstas consiste en 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" (tratamiento informático leal y legítimas; finalidades determinadas y legítimas; adecuados, pertinentes y no excesivos con las

finalidades; ser exactos y puestos al día, etc., art. 5 Ibídem) y "categorías particulares de los datos" [Prohibición al tratamiento informatizado de datos considerados *núcleo de la privacy*, salvo que se establezcan normas de protección apropiadas por los Estados. Art. 6 Ibídem] (art. 8, literal c).

La Directiva 95/46/CE, establece que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las *"decisiones individuales automatizadas"* en las que los Estados reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. (Art.15-1); que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado (Considerando 41);

El derecho de acceso a los datos, según la Directiva Comunitaria, se extiende a obtener del responsable del tratamiento, lo siguiente: 1. Libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: a) La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como la información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; b) La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; c) El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de "las decisiones individuales automatizadas", antes mencionadas. 2. En su caso, la *rectificación*, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular, a causa del carácter incompleto o inexacto de los datos; 3. La notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con lo previsto en el numeral anterior, si no resulta imposible o supone un esfuerzo desproporcionado (art.12).

Esto confirma que el derecho de acceso a los datos por una persona concernida lleva aparejado otros derechos previos, concomitantes y posteriores. En los primeros se ubica el

derecho a la información que tiene toda persona titular de los datos en cualquier fase del ciclo informático. Entre los segundos están, el derecho de rectificación y *bloqueo de datos* (jurídicamente una especie de medida cautelar suspensoria en tanto se resuelva una instancia, recurso o procedimiento previos), por ser incompletos o inexactos; y en los últimos, se ubica el derecho resultado de los anteriores, es decir, el derecho de actualización y puesta al día de los datos.

A pesar de todo, el derecho de acceso, como todos los derechos previstos en las normas comunitarias y constitucionales estatales, no es absoluto sino limitado a otros derechos de igual rango, al ordenamiento jurídico ("reserva de ley") e intereses colectivos. En tal virtud, la Directiva prevé una serie de excepciones y limitaciones al derecho de acceso, considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información (considerandos 42 y 44).

Las excepciones como las medidas legales para limitar el alcance de las obligaciones y derechos continentes y contenido del derecho de acceso a los datos personales, podrán establecerse según la Directiva Comunitaria, como medidas necesarias 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) un 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 c, d, y e, anteriores; y g) la protección del interesado o de los derechos y libertades de otras personas. Igualmente, se podrán utilizarse medidas apropiadas para limitar el derecho de acceso a los datos de "personas concretas", cuando no exista riesgo de atentado contra la intimidad del interesado, los datos se vayan a tratar excesivamente 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 (art. 13).

Este marco amplio y casi nugatorio del derecho de acceso a los datos personales por parte del concernido se ve equilibrado por el derecho que la legislación comunitaria denomina "*Derecho de oposición del interesado*" (art.14) consistente en que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad

pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias (considerando 45). Este derecho de oposición junto al derecho de *habeas data* conforma la estructura vertebral de la visión iusinformática de los derechos fundamentales (incluido el derecho a la intimidad) previstos en las Constituciones de los Estados modernos, tal como hemos analizado en la Parte I. [211].

5.2.1.3.2. LA FASE ESPECIAL O FASE OUTPUT DE DATOS. EN ESPECIAL "EL FLUJO INTERNACIONAL DE DATOS".

El Convenio Europeo de Estrasburgo de Enero 28 de 1981, en su parte considerativa dedicó su espacio exclusivamente al fenómeno hoy conocido como "Flujo internacional de datos" o "flujo transfronterizo de datos", como lo nominaba éste Convenio, por entender con sobradas razones sus creadores que en la circulación de los datos de carácter personal, por vías, espacios y tiempos electrónicos generan una amplia amalgama y paradoja de protección, garantía y vulnerabilidad de derechos, libertades e intereses legítimos. En efecto, se sostuvo:

> *El fin del Consejo de Europa es llevar a cabo 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;*
> *Considerando que es deseable 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;*
> *Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras;*
> *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,*

El Convenio Europeo de 1981, al abordar el tema de los flujos electromagnéticos de datos personales entre los Estados, evidenció aún más los constantes, penetrantes y porosos medios informáticos, electrónicos o telemáticos que desde aquella época se vienen utilizando por personas naturales, jurídicas, públicas y privadas para transferir, ceder, recuperar o simplemente consultar por mera visualización en pantalla o por medios idóneos *a posteriori,* guardados previamente en memoria principal o auxiliar en unidades centrales o periféricas de software y hardware. Juntamente con ello, puso en evidencia los contenciosos surgidos de uno de los últimos tópicos del poder (el derecho a la información) nacido de las tecnologías TIC y la

---

(211) 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* "Considerando que los principios de la protección 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- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas 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 (Considerando 25). Cfr. AA.VV. DISCOS COMPACTOS CELEX, Bruselas, 1997.

informática: derechos, libertades públicas e intereses legítimos, protección y garantía estatales y cuadro de límites y excepciones para mantener equilibrios.

El profesor *Poullet* **[212]**, define a los "flujos transfronterizos de datos" sólo dentro de la concepción del Convenio de Europa, como "la trasmisión personal o de las informaciones a través de las fronteras políticas y culturales, por el procedimiento de aprovisionamiento en las filas de computadores". Por su parte, *Van der Mensbrugghe*[213], exalta la conceptualización de Poulet, cuando señala que la transferencia o intercambio de datos

> *es vital entre las oficinas de la información, no únicamente por el aporte en el crecimiento internacional de la producción, sino por cuanto facilita la competitividad y la no discriminación. Además es necesario reconocer la interdependencia entre oficinas que tienen incorporada en sus estructuras la informatización de los datos. La importancia de la internacionalización de datos se refuerza por el aumento de los ficheros informatizados y la progresión rápida y sorprendente de las tecnologías.*

El Convenio Europeo, con base en los considerandos iniciales mencionados reguló en forma específica, en su articulado, todo lo atinente a los "Flujos transfronterizos de datos", pero especialmente, el intercambio electrónico de los datos de carácter personal proporcionando una serie de directrices normativas sobre la materia para los diferentes Estados Europeos suscriptores del Convenio. Sin embargo, dichas guías se plantearon, en parte (nos referimos a la técnico-jurídica que regulan a los mecanismos "de intercambio electrónico de datos" --EDI--, como anteriormente se ha visto), dentro de una lógica tradicional cuando se hace mención a los "flujos transfronterizos", recordando los límites geográficos que en la "cultura electrónica" desaparecen. Olvidan los redactores del Convenio que los fenómenos electromagnéticos TIC, se caracterizan principalmente, como lo sostiene el profesor Ethain, por realizarse dentro de marcos, formatos, velocidades electrónicas y sin contextuación de los espacios geográficos. Si el flujo de datos se hace por soportes y medios que no sean los electrónicos, la lógica empleada por el Convenio en este punto es explicable.

Las directrices sobre los flujos electromagnéticos de datos, según el Convenio son: a) Las disposiciones normativas del Convenio se aplicarán a las transmisiones a través de "las fronteras nacionales", por cualquier medio que fuere (a nuestros efectos,

---

(212) Citado por Patricia VAN DER MENSBRUGGHE. En: FLUJOS TRANSFRONTERIZOS DE DATOS EN LA DIRECTIVA 95/46 DE LAS COMUNIDADES EUROPEAS. En: Revista Actualidad informática Aranzadi. Ed. Aranzadi S.A., No. 20 Julio, Elcano (Navarra), Madrid, 1996, pág. 12

(213) Vid.VAN DER MENSBRUGGHE, Patricia.. En: FLUJOS TRANSFRONTERIZOS... Ob. cit. pág. 13

sólo los electromagnéticos), de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento; b) Un Estado no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial "los flujos transfronterizos" de datos de carácter personal con destino al territorio de otra Parte (art. 12-1 y 12-2); y c) Aplicación de los principios y derechos de protección y seguridad de los datos personales en todo intercambio electrónico de datos por parte de los Estados, autoridades "controladoras"; y en general por personas naturales, jurídicas, públicas o privadas.

Estas reglas generales, sobre todo las estipuladas en el literal b, en vigencia del Convenio se estableció como contrapartida una serie de excepciones, siempre y cuando se den unas condiciones y requisitos. En efecto, se aplicarán como excepción al flujo electromagnético de datos personales, con el fin de proteger la intimidad de la personas y los demás derechos fundamentales --como debió ratificar el Convenio--[214], cuando:

a) la legislación interna de los Estados prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros informatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente; b) cuando la trasmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo (art. 12). Estas excepciones tienen como fundamento el principio de protección equivalente y proporcional de los datos personales y el principio de negación de los Estados que se han considerado por el profesor *Morales Prats* [215] como "*paraísos informáticos*", por no tener regulaciones normativas compatibles en sus ordenamiento jurídicos vigentes que protejan los derechos, libertades públicas e intereses legítimos de las personas. Sin embargo, siguen existiendo paraísos informáticos, aún teniendo cimeras estructuras normativas de protección de datos personales sometidos a sistemas y tratamiento informatizados, a

---

(214) Y los demás derechos fundamentales previstos en las Constituciones de los Estados, decimos, aunque esto no lo previera expresamente el Convenio, pues creemos que el derecho a la intimidad no es el único que puede resultar vulnerado en una trasmisión o intercambio de datos personales, tal como lo hemos sostenido en otra parte de nuestro trabajo, al comentar el Documento Electrónico (EDI). Bástenos mencionar que el habeas Data, en muchas ocasiones se ve seriamente implicado por activa y por pasiva. Véase además, Punto 4 y ss. 4.3 Parte III.

(215) MORALES PRATS, Fermín et all. *COMENTARIOS A LA PARTE ESPECIAL DEL DERECHO PENAL. En:Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio.* Ed. Aranzadi, S.A. Pamplona, 1996, pág. 319

través de soportes y medios informáticos, electrónicos o telemáticos, en donde todavía se transita en ambientes tradicionales, dentro de una cultura del mundo escrito o del impreso, muy a pesar de la fuerza de choque y ruptura que encarna la "cultura electrónica". v. gr. El caso Norteamericano. Los recientes casos judiciales todavía contables con los dedos de la mano, ventilados ante los Tribunales de Justicia y Corte de Apelaciones de los EE.UU, originados en la indebida, ilegal o delictual utilización de soportes y medios informáticos, electrónicos y telemáticos por personas naturales y jurídicas (privadas y pública), comentados a lo largo de esta investigación. En otros Estados del mundo que tienen normas jurídicas sobre protección de datos personales, no se conocen aún casos sobre estos asuntos.

Por su parte en la E.de M., de la LORTAD y el propio cuerpo normativo de ésta **[216]**, hacen mención al "Movimiento internacional de datos", para referirse a la transferencia o flujo electromagnético temporal o definitivo de los datos personales tratados desde la fase inicial o de *input de datos* hasta su almacenamiento y registro con soportes y medios informáticos, electrónicos y telemáticos. La E.de M., sostiene:

> *la trasmisión internacional de los datos. 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.*

La transposición del art. 12 del Convenio Europeo de 1981, en el seno de la LORTAD, implica, entre otros efectos jurídicos y materiales, que tanto la conceptualización de "flujo transfronterizo de datos", como las condiciones o requisitos para transferir entre Estados datos de carácter personal para garantizar y proteger los derechos, libertades públicas e intereses legítimos

de las personas, tales como el de la intimidad, de la información (*habeas data* en su conjunto), etc., constituyen la regla general que contiene excepciones. En efecto, la transposición de la normativa implica efectos por activa y por pasiva. Se garantizan y protegen derechos fundamentales, pero a la vez, se recuerda que éstos tienen como característica esencial en su constitución el

---

(216) Cfr. AA.VV. *COMPENDIO DE DISCOS ARANZADI...* Ob. cit., 1997

de no ser derechos absolutos, o lo que es lo mismo, que son derechos limitables por otros derechos de igual rango, por los ordenamientos jurídicos de cada Estado e incluso por los intereses de la comunidad donde se van a aplicar. Esta transposición normativa en definitiva es total, sin reserva legislativa alguna [**217**], pues como se sostiene en la E.de M., de la LORTAD, se trata con la transposición de abarcar todos las "previsiones de los instrumentos internacionales como los Acuerdos de Schengen o *las futuras normas comunitarias"*. Y en efecto, estas normas futuras vinieron con la expedición
de la Directiva 95/46/CE, como veremos *ut supra*.

La LORTAD, establece como norma general, que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas (art.32).

La LORTAD, responde así a los criterios utilizados por el Derecho comparado para este supuesto (exigencia del consentimiento del afectado, condicionamiento de la trasmisión a que el país o la organización receptora ofrezcan garantías suficientes de protección o al grado de ´sensibilidad´ de los datos, así como a la constancia de una intervención administrativa al efecto [**218**].

Como excepciones a la regla prevista en la LORTAD, se establecen cuatro grupos de situaciones en las que no cabe la aplicabilidad del flujo electromagnético de

---

(217) La transposición de una norma, debe evaluar, entre otros aspectos, la situación legislativa actual sobre la materia en el Estado receptor de la transposición, las deficiencias y fortalezas normativas, las principales consecuencias en el marco legislativo, o también como sostiene el profesor *J.Dumortier y Diana M. Alonso Blas*, se sopesará el ámbito de aplicación territorial y temporal de la norma, el marco de principios, derechos y obligaciones garantizados y protegidos, las excepciones y limitaciones a los derechos fundamentales; y por su puesto, las "Reglas para las transferencias internacionales de datos". Vid. DURMOTIER, J.

y ALONSO BLAS, Diana M., *LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION DE DATOS EN BELGICA. En: Actualidad informátoca Aranzadi.* Ed. Aranzadi, S.A. Pamplona, Núm. 20 , Julio de 1996, pág. 1 y 7 y ss.

(218) El autor citando a *Dresner,* expone como en el derecho comparado dicha "constancia" exigida por la LORTAD, en este punto, en otras latitudes como Suecia se requiere "autorización de la exportación" o mera notificación (Noruega), declaración de un registro (Francia y Reino Unido), mera garantía del derecho de acceso y rectificación en los registros (Alemania). Creemos que la opción que más se acerca a la "cultura" y fenómeno del flujo electrónico de datos es la que sigue la legislación Alemana, pues las otras siguen en el esquema de transferencia de datos como una especie de correo tradicional, y esto no es así. Véase, SOUVIRON, J.M. *EN TORNO A LA JURIDIFICACION DEL PODER...* Ob. ut supra cit., pág. 169-170.

datos personales. En efecto, estos son: a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España; b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional; c) Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos; y, d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

En la doctrina española este cuadro de excepciones no tiene reparos, aunque si se hecha de menos, en el caso de la excepción del literal a), que España no exija al receptor de la transferencia electrónica de datos personales que "ofrezca garantías de protección suficientes" en el caso de los ficheros de titularidad pública **[219]**. Sin embargo, es comprensible que siendo Tratados o Convenios bilaterales o multilaterales, según el caso, las exigencias, derechos, obligaciones, excepciones y limitaciones de derechos que estos contengan deben ser recíprocas y no simplemente exigencias de una de las partes involucradas en el negocio jurídico internacional.

Finalmente, cabe resaltar que la LORTAD al mencionar "Movimiento" por "Flujo", transferencia o intercambio de datos personales involucra una acción electromagnética de trasmisión de datos (emisión y recepción), en la cual por obvias razones no tiene porque destacar fenómenos de la cultura tradicional mercantilista de exportación o importación de datos, tal como lo pretende *Piñol y Souvirón* **[220]**, pues como se ha insistido tantas veces el intercambio electrónico de datos (Documentos EDI), incluye la emisión como la recepción dentro de una lógica electrónica de las nuevas tecnologías de la información o comunicación (TIC).

La Directiva 95/46/CE., al abordar el tema del flujo electromagnético de datos personales hace referencia a la "*Transferencia de datos personales a países terceros*" (art.25), explicando previamente en los considerandos de la Directiva que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que 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 (C. 56). Es decir, que se exalta la necesidad imperiosa por parte de los Estados Miembros de

---

(219) Vid. SOUVIRON, J.M. Ob. ut supra cit., pág. 170.
(220) Ibídem, pág. 170

la UE., de contemplar la figura del flujo electromagnético de datos personales, con clara observancia de las garantías y niveles y grados de protección de los derechos, libertades públicas e intereses legítimos y las correspondientes acciones para implementar y potenciarlas por los Estados.

Así mismo, se considera necesario garantizar un *mínimum* de excepciones a la regla general del flujo electromagnético de datos en ciertos casos previa y taxativamente enunciados, tales como cuando se esté ante el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, 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.

Bien es cierto, que la Directiva actualiza jurídica como tecnológicamente el concepto de flujo electromagnético de datos personales, pero no cabe duda también, que éste cuerpo normativo comunitario recoge los elementos de conceptualización, estructuración y aplicabilidad suministrados desde la incorporación a la legislación europea del Convenio de Estrasburgo de 1981, sobre la materia. Sin embargo, cabe destacar de la Directiva el cuadro amplísimo de excepciones que establece la Directiva, no para aquellos Estados cuya transferencia de datos tenga por objeto tratamiento informatizado o se destinen a ser objeto de tratamiento informatizado, entre países que "garanticen un nivel de protección adecuados" (art. 25-1), sino para aquellos países que no ofrecen dichos niveles adecuados de protección (art. 26), confirmándose con ello que cada día se impone "*la libre circulación de los datos*"[221] frente a los regímenes

(221) Quizá lo más destacable de la Directiva sea precisamente la reglamentación, protección y garantía de uno de los principios-derechos más importantes del tratamiento informatizado, cual es, la "*libre circulación de los datos*". Por ello, la Directiva 95/46/CE, en su epígrafe intitula: " ...protección de las personas física en lo que respecta al tratamiento de datos personales y a la circulación de estos datos". Es un principio programático presente en todo el procedimiento informatizado de datos personales y un derecho fundado en el tríptico de derechos consecuentes del habeas data (derecho de acceso, rectificación y (continua)

normativos que previeran excepciones de índole negativa al ejercicio del derecho de acceso a la información o datos personales contenidos en ficheros o bancos de datos.

De esta forma, la Directiva establece reglas claras con respecto a las transferencias internacionales de datos: total libertad dentro de la Comunidad y prohibición (con ciertas excepciones, recogidas en el art. 26) cuando se trata de países terceros que no garanticen un nivel adecuado de protección [222]. Sin embargo, es lo cierto, que la mencionada prohibición frente al cúmulo de excepciones queda desvirtuada, pues tantas y de tal envergadura que bien puede afirmarse que el principio-derecho de *libre circulación de los datos* esta garantizado tanto en la Comunidad como en el resto de Estados del mundo, sólo que estos últimos deben demostrar que se encuentran bajo el abrigo de una de las variopintas excepciones que veremos más adelante.

Aunque claro está, como especie de reserva normativa de carácter preventivo y en cierto modo de temor a una liberación total del principio-derecho de libre circulación de los datos para terceros países, se establece un criterio directriz para evaluar previamente el carácter de "*nivel adecuado de protección*" por parte de los Estados transmisores (emisor/receptor) de los datos personales.

En efecto, el carácter de nivel adecuado de protección se debe evaluar *a priori*, por el Estado involucrado, "atendiendo a todas las circunstancias que concurran en un a transferencia o en una categoría de transferencia de datos; en particular se tomará en consideración 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); es decir, analiza, evalúa y decide todas las circunstancias de modo, tiempo y lugar de la transferencia de datos personales: sí son datos personales generales o componentes del llamado *núcleo esencial de la privacy*; y sobre todo, si existe normas idóneas de protección y seguridad en la transferencia de datos. Esta protección y seguridad últimas

Continuación cita No. 221

actualización y cancelación de datos o informaciones). Sobre este aspecto, la Directiva es insistente en los considerandos al exponer esta doble visión (principio-derecho) de la "libre circulación de los datos" (considerandos 3, 6, 8 y 9) y propugnar porque todo los Estados miembros de la UE, implementen todas las medidas jurídicas y técnicas (relativas a las nuevas tecnologías TIC e informática: software y hardware) necesarias para eliminar los obstáculos a la libre circulación, transferencia, y por ende acceso a los datos personales.

(222) Vid. DUMORTIER, J., y ALONSO BLAS, Diana M. *LA TRANSPOSICION DE LA DIRECTIVA DE PROTECCION*.... Ob. cit. ut supra cit., pág. 11.

están rectamente dirigidas a las medidas necesarias que deben adoptar los Estados en la transferencia, tanto de tipo jurídico como tecnológico (soportes y medios de software y hardware).

Las excepciones en cascada, por niveles y rigurosamente condicionadas y previstas en el art. 26 de la Directiva 95/46/CE, tienen a proteger no a los Estados involucrados en la transferencia de datos personales, sino esencialmente al principio-derecho de la *libre circulación de datos*, que implica la protección y garantía de un grupo de derechos entre los que están los de *habeas data y la intimidad* (aunque indistintamente se use por la Directiva, "vida privada" o intimidad).

Se podrá transferir entre Estados, datos personales aún no teniendo uno de éstos niveles adecuados de protección, siempre y cuando: a) el interesado haya dado su consentimiento inequívoco a la transferencia, 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 de defensa de un derecho en un procedimiento judicial, e) la transferencia sea necesaria para la salvaguarda 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.

PARTE IV

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

1. NOTAS PRELIMINARES.

A partir de la segunda mitad del presente siglo --lo cual era presumible, después de la barbarie de la II guerra mundial--, la preocupación de las políticas criminológicas de los Estados Democráticos y de Derecho, por la vulneración de los derechos humanos continua e insistentemente tabuladas, evaluadas y analizadas por los criminólogos alemanes, italianos, centroeuropeos y americanos, dejaron de priorizarse, casi única y exclusivamente con base en las convencionales delincuencias de Asangre@, las Apatrimoniales@ o cualquiera otra que atentara contra un bien jurídico protegido y protegible tradicionales, tal y como se puede constatar con la simple lectura de los diversos catálogos punibles de los Estados modernos incluídos los del derecho consuetudinario anglosajón o los del ámbito de la *Common Wealth* en sus A Crimes Act@ [1].

En tal virtud, las nuevas preocupaciones; entre muchas otras, pero especialmente las devenidas del fenómeno tecnológico de la información y comunicación por medios electromagnéticos (informáticos y/o telemáticos) , se reflejaron en la doctrina de criminólogos y iuspenalistas, con carácter correctivo, represivo y punitivo y acogido inmediatamente por los Estados en sus diferentes leyes especiales y diversos Codex penales, antes que con carácter preventivo y civilista, en las normas administrativas, las cuales paradójicamente, fueron adoptadas por varios Estados cuando ya se habían expedido estatutos penales que reprimían la actividad

---

(1) Nos referimos a los Estados de *la Commonwealth* que siguen las sugerencias, recomendaciones y aplicaciones de la legislación comunitaria en las variadas actividades humanas objeto de su regulación normativa, Aen los cuales a falta de una base jurídica rígida de asociación está ampliamente compensada por los vínculos de origen común, historia, tradición jurídica y solidaridad de intereses@, como lo sostiene *Oppenheim.* T.I., p.224. Algunos de los muchos países que hacen parte de esta comunidad de Estados son: Inglaterra, Canada, Australia, Irlanda del Norte, Nueva Zelandia, etc. A título de ejemplo: La ACrimes Act 1914" de Australia. Texto de la ley tomado de: AA.VV. ***Base de datos de la Universidad de Australia.*** Legislación y datos vía Internet (WWW.AUSTLII.EDU.AU. Inglés), p.1.

humana a través de equipos computacionales o telemáticos, en sus múltiples formas y pretendían proteger y tutelar derechos fundamentales, como la intimidad, la honra, la imagen, etc., o bienes jurídicos específicos, como los patrimoniales y socio-económicos [2].

Las nuevas actividades humanas transgresoras de derechos fundamentales no patrimoniales (también llamados de la persona o la personalidad) y patrimoniales --se sostiene--, cobraron relevancia con el surgimiento de la tecnología informática [3], el multitratamiento de la información y la comunicación por medios electrónicos, por el avance y gran poder de la teletransmisión de datos sin fronteras [4]; la excesiva libre oferta-demanda de equipos computacionales personales (o Apersonal computer@-PC- u Aordenadores@ [5]), corporativos o empresariales e incluso industriales (Ahardware@: unidades de procesamiento y periféricas [6]); y sobre todo, por el fácil acceso, tratatratamiento, uso y abuso de programas

---

2) Mi escrito intitulado: ***La Constitución de 1991 y la informática jurídica.*** Ed.UNED, Pasto (Col), pág. 124 Para indicar que el fenómeno de la informática lo invadió todo, tan rápidamente como ninguno otro la había hecho, y en consecuencia, los Estados en la práctica no pudieron hacer lo que en teoría era previsible, es decir, regular normativamente, cuando menos, el acceso, tratamiento y uso de la informática en todas las actividades humanas, sin recurrir a la *ultima ratio* para reprimirla pues los hechos de la vida cotidiana en los que estaba involucrada la informática había desbordado el fenómeno mismo y por supuesto, cualquier tentativa de regulación preventiva, civilista e institucional de carácter administrativo resultó para muchos Estados como Colombia, al menos poco oportuna, eficaz y de verdadera política-estatal contra los nuevos fenómenos tecnológicos, a pesar de que se advertía en la Constitución Política (art. 15) de los Ariesgos@ sobrevinientes de la informática contra los derechos fundamentales.

(3) En éste sentido: BUENO ARUS, Francisco. ***El Delito Informático***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 11 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1994., pág.1 y ss. MORALES PRATS, Fermín. *El descubrimiento y revelación de Secretos.* En: ***Comentarios a la Parte Especial del Derecho Penal***. Ed. Aranzadi, Pamplona (Esp.), 1996, pág. 297. También: en ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp), 1984, pág.33 DAVARA R. Miguel. *Manual de Derecho Informático.* Ed. Aranzadi, Pamplona (Esp.), 1997, pág.285 y ss. CARBONELL M., J.C. y GONZALEZ CUSSAC., J.L. ***Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio***. En: Comentarios al Código Penal de 1995. Vol. I., Ed. Tirant lo blanch, Valencia (Esp.), 1996, pág. 999 y ss. HEREDERO HIGUERAS, Manuel. ***La protección de los datos personales registrados en soportes informáticos*** .En: Actualidad Informática Aranzadi. A.I.A. Núm. 2, Enero, Ed. Aranzadi, Elcano (Navarra.), 1992. págs. 1 y ss.

(4) Veáse, NORA, Simón y MINC, Alain. ***Informe nora-minc. La informatización de la sociedad.*** Trad. Paloma García Pineda y Rodrigo Raza, 1a., reimpresión. Ed. Fondo de Cultura Económica. México-Madrid-Buenos Aires, 1982, págs. 53 a 115. Más Recientemente, ***La Directiva de la Unión Europea 95/46/CE, del Parla- mento 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.*AA.VV. ***Base de datos Acelex@.*** Ed. Comunidad Europea, Bruselas, (B), 1997., pág. 20

(5) La traducción del término francés AOrdenateur@ al castellano AOrdenador@, es el que se ha impuesto en la legislación, doctrina y jurisprudencia españolas, en tanto que el término inglés Acomputer@ (Acomputador@), es el que se ha aceptado en un amplio sector del mundo.

(6) La Unidad de Procesamiento Central *(Central Processing Unit*, CPU), que es como el Acerebro@ del computador, pues allí se desarrolla el principal trabajo electromagnético y mecánico. En términos sencillos, es la parte del computador que hace posible la emisión y recepción o tratamiento propiamente dicho de la información. Esté como las unidades periféricas, o también llamados Asoportes informáticos@, son aquellas partes que rodean, auxilian, complementan y confirman un

procedimiento informático (monitores, teclados, discos, impresoras, etc). A todo esto, se denomina Hardware básico o primario. Vid. Mi trabajo. ***La Constitución de 1991 y***... Ob. ut cit.págs. 128 a 242.

computacionales o Asoftware@, los Aficheros@ [7] o bases de datos (de toda clase, fin, servicio y origen público o privado, existentes), por parte de las personas sin distingo de edad o parámetro de distinción alguno, con autorización o sin ella.

2. REGULACION IUSPENALISTA DEL DERECHO DE ACCESO A LA INFORMACION, EL HABEAS DATA Y LA INTIMIDAD.

El proceso de tratamiento informatizado de la información o de los datos de carácter personal, comporta una serie de etapas, fases o ciclos informáticos, tal como hemos analizados en la Parte I y III de esta investigación. Las diferentes legislaciones del mundo han regulado este procedimiento informático desde el punto de vista del derecho administrativo y civil y para protegerlo como *ultimo ratio*, en todo o en parte, se han añadido mecanismos jurídicos de tipo penal, para tutelar los derechos al acceso a la información, las facultades estructurales del *habeas data* (conocimiento, actualización, rectificación y cancelación de datos); y por su puesto, los derechos y libertades fundamentales, tales como la intimidad.

El derecho de acceso a la información que tiene toda persona se encuentra regulado en las diversas constituciones del mundo como un derecho fundamental y personalísimo e indefectiblemente se halla vinculado con otros no menos importantes y de igual rango constitucional, como el derecho a informar y ser informado y el derecho a la intimidad personal y familiar, tal como sucede en España y Colombia (v.gr. arts. 18 y 20.1.d) CE., y arts. 15 y 20 Cons.Col.). Hoy por hoy, en la llamada *era de la informática*, el derecho de acceso a la información adquiere relevancia capital que oscila entre el mayor o menor grado de poder de control sobre los datos o informaciones que conciernen a las personas cuando se hallen almacenados, registrados, conservados o

---

(7) AFichiers@, es la versión francesa de la castellana AFicheros@. En la versión inglesa son ABanks@. Una y otra se entiende como un conjunto coherente de datos personales que previo un tratamiento informatizado (Ain@), pueden ser accedidos o recuperados (Ainput@ or Aoutput@), por las personas interesadas o terceros, o por los responsables de su vigilancia y control, cuenten o no con autorización para hacerlo. La disyuntiva de la autorización o no marca la licitud o ilicitud en el acceso, uso o conservación.

transmitidos por medios informáticos, electrónicos o telemáticos por personas naturales, jurídicas, públicas o privadas, según fuere el caso. En dicho marco, se produce el binomio derecho-protegido y derecho-vulnerado y el correspondiente equilibrio ponderado que deviene principalmente de los límites constitucionales y legales de los derechos y libertades fundamentales en éste involucrados y que tanto hemos comentado a lo largo esta investigación.

Los diversos Estados, tras constitucionalizar el derecho de acceso a la información y el habeas data, han optado por la técnica legislativa para cumplir con su papel proteccionista o garantísta del conjunto de derechos y libertades fundamentales.

En efecto, así se ha procedido en el Canadá al emitir leyes que regulan los derechos de acceso a la información y el derecho a la intimidad (Access to information Act, 1980-1983; Privacy Act 1980-83), igual en Australia (Freedom of information Act 1982, complementada por la Privacy and Data Protection Bill, 1994 -NSW- Privacy Act, 1988) [8]; en Alemania (Ley Federal Alemana de Protección de Datos, Enero 27 de 1977, reformada el 20 de diciembre de 1990); en España (Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal o LORTAD, L.O.5/92, Oct. 29. Reglamentada por el R.D.1332/1994, de 20 de Junio. Ley 30/1992, Ley de Régimen Jurídico de las Administraciones públicas y procedimiento administrativo común. LRJPA, arts. 37 y 45, sobre *documentos informáticos, electrónicos y telemáticos* y el R.D. 263/1996, Feb.16.,sobre la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. Además las normas comunitarias sobre la materia v.gr.Convenio de 1981 y la Directiva 46/95/CE), y en Colombia [9].

---

(8) AA.VV. Base de datos de la universidad de Montreal (Canadá). Departamento de Derecho Público. Biblio teca Virtual (Inglés-Francés). Vía Internet (WWW.UMONTREAL.EDU.CA), págs. 1 y ss. AA.VV. Base de datos de la universidad de Australia. Vía Internet. (www. austlii.edu.au), págs. 1 y ss.

(9) Estatuto del derecho a la información: Ley 57 /85, de 5 de Julio, Código Contencioso Administrativo y el Reglamento aprobado por la Junta Directiva de la Asociación Bancaria y de Entidades Financieras de Colombia, de 23 de Marzo 23 de 1995, relativa a la *información económica y financiera* sometida a tratamiento y procedimiento informatizado de carácter privada con competencias sólo de buena gestión y manejo del sistema informático, creado o puesto en funcionamiento por la Central de Información de ASOBANCARIA --CIFIN-- , pero no de sanción. En consecuencia, la Superintendencia Bancaria no tiene funciones de control, gestión, ni mucho menos de sanción sobre los bancos de datos que la CIFIN gestiona, Ani de las personas que lo administran, pues se trata de personas jurídicas diferentes a las vigiladas, a las

cuales prestan su servicio para la evaluación del riesgo de su clientela@(CC. Sent. T-486/1992, de 11 de Agosto. Sent. T-414/1992,de 16de Junio). Textos completos en WWW.RDH.GOV.CO. 1998.

Toda esta normatividad que concatena, a nuestros efectos, los derechos de la información, el habeas data y la intimidad en los diversos Estados constituye además, el cuerpo legislativo complementario, de interpretación y hermenéutica del derecho punitivo o de Anormatividad extrapenal@ [10] ,y por tanto, de ineludible observancia.

En el ámbito penal y como *ultima ratio*, los Estados mencionados, han previsto normas específicas en sus códigos penales para reprimir las conductas que se realizan con medios o equipos electromagnéticos, computacionales o telemáticos que atenten contra bienes jurídicos no patrimoniales o derechos fundamentales como el de acceso a la información o *habeas data*, la intimidad personal y familiar, la propia imagen, el honor; entre muchos otros, o también cuando atente contra bienes patrimoniales genéricos o de tratamiento jurídico *sui géneris* como la Apropiedad intelectual e industrial@.

Los Códigos Penal español y canadiense hacen referencia específica a la intimidad como bien jurídico protegido, aunque con diferente visión y cobertura de protección estatal según las fases del tratamiento electromagnético de la información, como en seguida puntualizamos.

Por su parte, el Código Penal Canadiense en el Tít. VI AInvasion Privacy@ (arts. 183 a 196), extiende la protección penal a la intimidad desde la fase de primaria o A*input*@ de datos (recolección), la fase *Ain*@ o de tratamiento electromagnético propiamente dicho (almacenamiento, registro y conservación de datos) hasta la fase A*output*@ de la información (comunicación: emisión/recepción de datos). Los delitos utilizando medios manuales, mecánicos , informáticos o telemáticos o la información misma como objeto material de los estos, son: 1. Interceptación de datos o informaciones de particulares, sin su consentimiento (art. 184); 2. Interceptación de datos consentida por una de las partes (art.184.1 y 2) y/o por telecomunicaciones u otros medios tecno-

---

(10) MORALES PRATS, Fermín. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. En: Comentarios a la parte especial del Derecho Penal. Dirigida por Gonzalo Quintero Olivares y Coordinada por José Manuel Valle Muñiz. Ed. Aranzadi, Pamplona (Nav.), 1996. pág. 309 y ss.

lógicos (art.184.3); 4. Interceptación judicial de datos en circunstancias excepcionales (art. 184.4); 5. Interceptación de datos o información a través de dispositivos electromagnéticos, mecánicos o telemáticos, con fines de lucro (art. 184.5); 6. Interceptaciones autorizadas (art. 185); 7. Interceptación por autorización judicial. Excepciones. (art.186); 8. Interceptación de un dato o información secreta o confidencial. Agravantes (art. 187); 8. Interceptación por autorización judicial en casos especiales (art. 188); 9. Posesión o compraventa de dispositivos electromagnéticos o informáticos utilizados en la interceptación subrepticia de datos. (Art. 191); 10. Descubrimiento o revelación de la información sin consentimiento con medios mecánicos, informáticos o electromagnéticos (art. 193); y, 11. Descubrimiento de datos o informaciones interceptadas, sin consentimiento, a través de medios electromagnéticos, mecánicos e informáticos (art. 193.1).

En España, el profesor *Morales Prats* [11], previa distinción de la fases del ciclo informático (recolección, registro o Aprogramación@, y transmisión de la información), confirma que la protección jurídico penal de los derechos fundamentales como el de la intimidad, la imagen e incluso el honor se extiende a partir del registro de los datos de carácter personal, es decir, a partir de la fase que llama de tratamiento o programación. En tal virtud, las fases previas a ésta (como la de recolección y almacenamiento de la información) se protegen o tutelan bien civil y/o administrativamente por las autoridades competentes. El autor citado, al comentar los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio, Tít. X, del C.P.del 95 (arts. 197 a 201), en forma prolija estudia la terminología técnica, jurídica e informática empleada en la regulación de las Ainfracciones administrativas@ previstas en la LORTAD (art. 42 y ss.) y los delitos del artículo 197.2, pues a su juicio, la LORTAD gana en identificación y precisión terminológica, de la que adolece el código penal, a tal punto que causa Aincertidumbre@ y A parece que el desconcierto y la precipitación han precedido la crea-

---

(11) MORALES PRATS, Fermín. ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp.), 1984. págs. 60 a 81. Ibídem. ***Delitos contra la intimidad...***.Ob. cit. pág. 312 y ss. Ibídem. ***Protección penal de la intimidad, frente al uso ilícito de la informática en el código penal de 1995.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, ADelitos contra la libertad y Seguridad@, Madrid, 1996. págs. 146 a 196 y ss. Sobre el tratamiento de datos (LORTAD y Dec.1332/94, Directiva 95/46/CE).

ción de éste precepto@ (art.197).

En consecuencia, la protección jurídica administrativa alude al momento mismo de la recolección y Aen forma especial por la salvaguarda de los derechos nucleares del *habeas data*, esto es, los derechos de información, acceso, rectificación y cancelación sobre los datos personales@, realizada por la Agencia Protectora de Datos Española, la cual entre otras facultades tiene, las de Apreventivas de control, supervisión e inspección que le otorga la LORTAD en el ciclo operativo del banco de datos@. *Arroyo Zapatero* [12], en esta mima línea de crítica, manifiesta que Ala tutela penal, para ser eficaz debería haberse extendido a todas las fases del ciclo informático, desde la creación de los ficheros informáticos hasta la alteración y transmisión ilícita de los datos registrados@. Sin embargo, con fundadas razones un sector de la doctrina española, reconoce que no es fácil para el operador jurídico distinguir , en este punto, los linderos entre infracción administrativa y delito cuando se atenta contra los datos de carácter personal o informaciones personales, a tal punto que se evidencia un cierto solapamiento en algunas acciones de origen aparentemente administrativo que en otras legislaciones han merecido tipificación penal [13], o más aún, cuando infracciones y sanciones administrativas [14] por su contenido son verdaderos delitos y penas [15], correspondientemente suavizados por la mano mágica de la naturaleza iusadministrativa.

---

(12) ARROYO Z., Luis. ***La intimidad como bien jurídico protegido*** . En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, AEstudios del Código Penal de 1995@, Madrid, 1995, pág. 306.

(13) MORALES P., Fermín . ***Delitos contra la intimidad...*** Op.cit., pág. 317.

(14) La protección a la Aprivacidad@ (por intimidad) es preventiva o cautelar y represiva, ambas de naturaleza administrativa, así mismo el carácter administrativo de las figuras cuasi delictivas previstas en los arts. 42 y 43 de la LORTAD, como Ainfracciones leves, graves y muy graves@, y sostiene que ésta Aparece haberse inspirado más bien en el criterio despenalizador de conductas reprochables a que responde@ y por ello, no se ha A tipificado ni una sola figura delictiva@, y finaliza Ala protección de carácter represivo que otorga la LORTAD es exclusivamente administrativo@. GONZALEZ NAVARRO, Francisco. ***Derecho administrativo español.*** Ed. Eunsa, Pamplona (Esp.), 1 ed., 1987, y 2 ed. 1994, p.179.

(15) Contrariamente a la tesis de González Navarro, el autor sostiene luego de enunciar algunas de las llamadas Ainfracciones leves, graves y muy graves@ previstas en 42 y 43 de la LORTAD, que dentro de Aéstas infrac ciones hay bastantes que, en realidad, por otra vertiente, constituyen delitos. De ahí la extremada gravedad de la actuación que se encomienda a la Agencia@ de protección de Datos, creada por la LORTAD, como organismo de conservación, control, vigilancia, investigación y sanción disciplinarias y de infracciones contra datos informáticos públicos y privados. Vid. FAIREN GUILLEN, Víctor. ***El habeas data y su protección actual sugerida en la ley española de informativa de 29 de octubre de 1992 (interdictos, habeas corpus)***. En: Revista de Derecho Procesal. Ed. de derecho reunidas, Madrid, 1996, pág. 542.

En los Códigos Penal Australiano y Alemán, relacionan las conductas humanas en las que se utilizan medios o equipos computacionales, electromagnéticos y telemáticos que atenta contra el *habeas data,* los datos de carácter particular y los datos o informaciones de valor Aeconómico@. En efecto, en el ACrimes Act 1914" Australiano (*Computer related Commonwealth law*) en la Parte VIA y VIB, arts. 76A a 76E y 85ZE, se relacionan los siguientes delitos (A*offence*@): 1. Acceso no autorizado a los datos; 2. Destrucción, modificación e impedimento de acceso a los datos; 3. Acceso no autorizado de los datos utilizando medios informáticos o telemáticos; 4. Destrucción, Modificación o impedimento de acceso a los datos utilizando medios informáticos y telemático; 5. Delito de hostigamiento (Adelito conductista@ behavorístico) mediante el uso de medios informáticos y telemáticos.

En Alemania, la denominada ASegunda Ley para la lucha contra la Criminalidad Económica (2.WIKG) de 15 de Mayo de 1986., relaciona una variada gama de hechos punibles cometidos con medios electromagnéticos o informáticos o de la información como bien jurídico u objeto material de los mismos, acorde con la realidad tecnológica en la que vivimos. En esta relación punitiva podemos encuadrar los *delitos contra los datos* o las informaciones, a diferencia de la legislación canadiense donde se destacan los *delitos de los datos* contra otro bien jurídico como la intimidad. La legislación española como veremos prevé una y otra clasificación [16] .

Las formas típicas del derecho alemán son: 1. Espionaje de datos (Arts. 202 a StGB); 2. Estafa informática (263 a StGB) ; 3. Utilización abusiva de cheques o tarjetas de crédito (266 b StGB); 4. Falsificación de datos con valor probatorio (269 StGB); 5. Engaño en el tráfico jurídico mediante elaboración de datos (270 StGB); 6. Falsedad ideológica (271 StGB); 7. Uso de documentos falsos (273 StGB); 8.Destrucción de datos (303 a StGB); y, 9. Sabotaje informático (303 StGB).

En Colombia, como precisaremos *ut infra,* el Código Penal de 1980 (C.P.Col)

---

(16) VALLE MUÑIZ, José Manuel y MORALES PRATS, F.,Ob.ut supra cit. Se refieren a los delitos contra el patri monio económico y contra el orden socioeconómico -- Tít.XIII-- (Delitos contra los datos) y los delitos contra la intimidad --Tit. X--, los relativos al ejercicio de los derechos fundamentales y libertades públicas --Tit. XXI, Cap. V-- y los previstos en leyes penales especiales. v.gr. La propiedad intelectual (Delitos de los datos).

no tiene referencia expresa, pero sí tácita al derecho de *Habeas Data* y/o a la intimidad como bienes jurídicos protegibles de cualquier atentado por parte de la informática o telemática dentro del género del bien objeto del Título X, ADe los Delitos contra la Libertad Individual y otras garantías@. En efecto, dos razones convincentes nos llevan a sostener este argumento: por una lado, debemos tener en cuenta que en una etapa de la evolución de los derechos fundamentales, éstos retomaron la configuración, estructura y contenido de las viejas Alibertades constitucionales@ del liberalismo clásico y postindustrial anglo-francés a la que no escaparon el habeas data y la intimidad, y por otro lado, tanto el derecho de *habeas data* como la intimidad o Aprivacy@, tienen hoy una identidad propia en la Constitución Colombiana de 1991 (art.15), a pesar de que el Código Penal todavía mantiene ese origen nominativo y genérico de ALibertades Públicas@ como bien jurídico protegible penalmente para referirse a una variopinta gama de derechos hoy considerados fundamentales dentro de los que están los mencionados.

En efecto, la Constitución, en el Titulo II, ADe los derechos, las garantías y los deberes@, Cap. I. ADe los Derechos Fundamentales@, art. 15, ADerecho a la intimidad personal y familiar@, constitucionaliza los derechos a la intimidad y el *habeas data,* al fusionarlos en un mismo artículo, bajo la fórmula siguiente: A *Todas las personas tienen derecho a su intimidad...Del mismo modo, tiene derecho a conocer, actualizar y rectificar las informaciones...*@ entendiendo el constituyente del 91, que éste último es una consecuencia lógica de la estructuración de la intimidad y no otro derecho también fundamental que tiene su sustento en el derecho a la información (art.20 y 73 ibídem), en el desarrollo de la personalidad (art. 16 id.) y en los valores constitucionales de la dignidad, respeto y solidaridad humanos (art. 1 id.) que no sólo a la intimidad puede servir de sustento, afección, restricción o límite o autolímite constitucional sino al cúmulo de derechos fundamentales previstos en el Título II de la Constitución, pues en un estado social de derecho y democrático no existen derechos absolutos. Por contra, la Corte Constitucional Colombiana estima que la intimidad es un derecho absoluto (Sent.T-022, Ene. 29/92).

Más aún, el artículo citado en el tercer inciso constitucionaliza el procedimiento o tratamiento automatizado de la información al decir: A*En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución@*, con lo cual no deja duda que el habeas data tiene identidad constitucional en el derecho colombiano y consagra derechos límitados por la propia constitución y los demás derechos.

Sin embargo, para seguir el hilo de este aparte digamos que el actual Código Penal de 1980, bajo el concepto genérico de libertades públicas subsume a la intimidad como bien jurídico protegible de cualquier conducta humana que utilice medios electromagnéticos, computacionales o telemáticos en el Título X, Cap.V., del C.P.Col., al referirse a los delitos de Aviolación de secretos y comunicaciones@, y en concreto, a: 1. La Aviolación ilícita de comunicaciones@ (art. 288); y, 2. La Aviolación y empleo de documentos reservados@ públicos o privados. Así mismo, por los delitos previstos en la legislación especial Decr. Ext. 2266 de 1991: Autilización ilícita de equipos transmisores o receptores@, incluidos los Aelectrónicos@ --informáticos o telemáticos--, (art.16), y Ainterceptación ilícita de correspondencia oficial@ (arts. 18) . La honra (art. 21 Cons. Col.) u Ahonor@, en el derecho español, también puede ser objeto de atentado de los medios tecnológicos de información y comunicación colectivos, y en tal virtud, se prevén los delitos de injuria y calumnia (arts.313 y ss del C.P. Col.), al estar incorporados en el bien jurídico tutelado de Ala Integridad Moral@.

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: Decs. 1355-2055 de 1970 y 522 de 1971, 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 tal virtud, siendo más graves las contravenciones especiales, se ha ubicado después de atribuir competencia a las autoridades administrativas locales y regionales, con funciones cuasi jurisdiccionales [17] y asignarles el conocimiento de las contravenciones Aque afectan la integridad personal@, la intimidad o la Avida íntima o privada de una persona@ (arts.46 a 49), cuando sin

---

(17) Véanse, mis trabajos: ***La jurisdicción civil de policía.*** Tesis para optar el título de abogado, Universidad de Nariño, Fac. de Derecho, Pasto, Mayo 27 1983, pág. 12 y ss. ***Constitucionalidad de la jurisdicción de Po licía*.** Monografía ganadora del AConcurso Centenario de la Constitución Colombiana de 1886". Banco de la República, Bogotá, 1984, pág. 18 y ss.

facultad legal se la averigüe hechos o datos de la intimidad, se los graba con cualquier medio tecnológico de información o comunicación que llama Asubrepticios@, o los Adivulga@ u obtiene Aprovecho@ de ese descubrimiento de información. Estas modalidades ilícitas se agravan si se hace a sabiendas, con conocimiento previo y sin justa causa..

3. LA INFORMATICA [18] JURIDICA DOCUMENTAL, El *HABEAS DATA* Y EL ESTADO.

Algunos Estados del mundo han constitucionalizado prematura o tardíamente Ael uso@, Ala aplicación@ o Ala utilización de la informática@ a los efectos limitar o restringirla con claros efectos proteccionistas o garantístas de derechos fundamentales, como en el caso de España, Colombia y Portugal, respectivamente. En efecto, se constitucionaliza para Agarantizar@ el derecho a la intimidad personal y familiar de los ciudadanos, la imagen, el honor y A el pleno ejercicio de sus derechos@, según la Constitución Española de 1978 (art. 18.4), o además de ello, para aplicarlo en el ejercer el derecho de *habeas data* (acceso, actualización y rectificación de la información) dentro del proceso de tratamiento electromagnético público y/o privado, que tiene toda persona, según la Constitución Colombiana de 1991 (art. 15); o más aún, como derecho fundamental aplicable todo Autilización de la informática@ y para prohibirla expresamente en el tratamiento de datos de carácter personal sobre aspectos filosóficos, de filiación política o sindical, de fe religiosa o vida privada Asalvo cuando se trate de procesamiento de datos de carácter estadístico no individualmente identificadas@, como en la Constitución Portuguesa de Abril 2 de 1976 [19].A este fenómeno constitucio- nalizador mundial sobrevino una creciente reglamentación legal para

---

(18) La STC 254/1993, Jul.20 y STC /1994, Mayo 9 de 1994. Sala 1. Se reconoce y destaca la importancia actual. Reconocimiento que ha sido reiterado por posteriores pronunciamientos del Tribunal Constitucio nal. STC Mayo 9 de 1994. TC1 y STC Enero 13 de 1998, TC1, FJ.4, en el cual se sostuvo: A Por su parte, la STC 254/1993, declaró con relación al art.18.4 CE, que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta contra la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (FJ.6). La garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data*) y comprende entre otros aspectos, la

oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél que justificó su obtención (FJ7).

(19) AA. VV. ***Constituçiâo Novo Texto.*** Ed Coimbra. Ediçâo organizada J.J. Gomes Canotilho o Vital Moreira, Portugal, 1982. pág. 29

completar el cuadro garantísta de los derechos fundamentales, tal como lo hizo España con cierta demora y excesiva buena expectativa frente al avance del fenómeno tecnológico de la información y la comunicación al expedir la LORTAD y su cascada de decretos reglamentarios[20], pues ya otros Estados del entorno europeo existían sus leyes con excesos o defectos, con falta de incardinación entre lo prematuro y lo desfazado del fenómeno tecnológico y las normas jurídicas por expedir; en fin, entre las experiencias para recoger o desechar al respecto. v.gr. Dentro de las normas prematuras, pioneras pero no sin defectos mínimos a la época están: La A*Data Lag*@ Sueca de 11 de Mayo de 1973; Las alemanas : a) *Land de Hesse* en Alemania, promulgada el 7 de Octubre de 1970; y, b) La Ley Federal de Protección de Datos de 27 de Enero de 1977, reeditada en la nueva Ley de 20 de diciembre de 1990; y más recientemente, La Ley francesa Arelativa a la informática y a los ficheros y las libertades@ de Enero 6 de 1978 y la Suiza de 16 de Marzo de 1981; entre muchas otras dentro y fuera del contexto europeo, como las citadas anteriormente de Canadá y Australia.

El art. 15 de la Cons. Col, en su parte inicial expresa: A*Todas las personas...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.@*, y más adelante complementa al indicar cuál es el procedimiento de recolección, tratamiento y circulación de datos o informaciones. Este fenómeno jurídico en la doctrina y legislación universal se ha conocido como *habeas data*, que algunos estados como los mencionados han elevado a rango constitucional en tanto que otros como España lo han reglamentado en la ley. Sin embargo, unos y otros reconocen su importancia capital en el juego pleno del respeto, protección y límites de los derechos fundamentales,

---

(20) La doctrina española era consciente de esa demora porque el entorno normativo europeo, así como la normativa de influencia en la UE (Unión Europea) establecía un status, unas directrices sobre regulación y protección en estas materias. V.gr., el Convenio de Europa de 1981, el cual, más tarde fuera retomada en la Directiva 95/46/CE, Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, sobre la Aprotección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos@. El profesor Davara, analiza el hecho de la demorada aparición de la LORTAD, explica que la demora no fue del todo buena, pues no se entiende todavía como persisten en ésta ley, Alas rígidas excepciones que se establece en ´favor´de los ficheros de titularidad pública y el ambiguo régimen y regulación del órgano de control --llamado Agencia de Control de Datos-- que crea la propia ley@. Vid. DAVARA R. Miguel. ***Manual de Derecho Informático.*** Ed. Aranzadi, Pamplona (Esp), 1997. pág. 70. En igual sentido: DEL PESO

NAVARRO, Emilio. ***La seguridad de la información.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 26 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1998, pág. 1 y ss.

además de considerar que las nuevas tecnologías de la información y comunicación (informática y/o telemática) están íntimamente ligados con éste fenómeno; y por eso, el carácter expresamente, y en no pocas veces, exageradamente proteccionista de los estados ante la irrupción agresiva de aquéllas, como no había sucedido desde las revoluciones postindustriales en el mundo.

En efecto, hoy más que nunca, se impone la pregunta:) Por qué la informática, revolucionó muchas facetas de la vida humana, en particular la visión del derecho penal y la actuación del Estado frente a éste?.

Las razones son variopintas, algunas de ellas las ha contestado el profesor *Hernández Gil* [21], al analizar el derecho, la informática y la ciencia y al encontrar que el derecho va experimentar un cambio en sí mismo, tras observar las nuevas realidades tecnológicas y el modo diferente en el que va a ser elaborado, tratado o conocido por éstas. El Tribunal Constitucional Español (STCS: 254/1993, Mayo 9/1994, Enero 1/1998); por su parte, ha evidenciado la importancia tras fijar el contenido esencial del derecho a la intimidad y de otros derechos fundamentales previstos en la CE, así como los límites constitucionales de existentes entre éstos y las posibles agresiones que pueden sobrevenir con las nuevas tecnologías de la información y comunicación (TIC): informática y/o telemática, tal y como concretaremos más adelante. Este repertorio de impactos tecnológicos no solo temporales sino de contenido han sido continuos, constantes y cada vez más sofisticados (v.gr. La Multimedia), estructura una nueva forma de estudiar, analizar y crear el derecho, y en particular en el ámbito penal. Así, el poder Asubversivo@ de la informática y telemática avanza acarreando consigo esa dicotómica consideración: por un lado, la de servir de vehículo actual, idóneo y visionario en la potenciación del tratamiento, procesamiento, divulgación o consulta de la información documentaria generada por el derecho, en general; y por otro, la de considerarse como una gran amenaza de carácter tecnológica en manos de quienes ilícitamente acceden, utilizan, usan, conservan o divulgan información o datos públicos o privados en contra de derechos y libertades públicas o bienes jurídicos.

---

(21) Citado en mi trabajo: ***La Constitución de 1991 y***... Ob. ut cit.pág. 51.

En efecto, con el advenimiento de las tecnologías de la información y comunicación (TIC), los juristas y el Estado mismo, comenzaron a replantearse la mejor forma de organizar el producto intelectivo de su actividad diaria (v.gr. Labor en oficinas particulares y públicas; el cúmulo de providencias judiciales, en el ámbito judicial; normas jurídicas, en el ámbito legislativo; normas administrativas, procedimientos gubernativos, estatutos, etc, en el ámbito administrativos, etc), cuando menos, en la parte más relevante de la información jurídica; es decir, en la que se crea, modifica, suspende o extingue derechos y/o libertades públicas, o que afectan directa o indirectamente aquéllas y persiguen su tutela y protección estatal. Toda esta Información años atrás se había mantenido en grandes soportes impresos o documentos escritos, en extensas bibliotecas generales y especializadas. Su incorporación, organización, conservación; y sobre todo consulta resultaba lenta, muchas veces engorrosa y de alta dosis de paciencia.

Como consecuencia, se buscó la mejor forma de ingresar, ordenar, clasificar y recuperarse el cúmulo de datos en forma automatizada (informática y/o telemática), a través del documento electromagnética, a fin de potenciar y eliminar la mayoría de obstáculos que representaba el documento impreso o escrito, y en realidad de verdad se consiguió en un alto porcentaje, no sin sacrificio, limitación o surgimiento de nuevas como variadas amenazas, principalmente a los derechos fundamentales o de expectativas *per se* devenidas de la tecnología, tal como analizó en el capítulo anterior, al comentar la informática jurídica documental [22], como parte de la informática jurídica.

Antes de la denominada época Apostindustrial@, no se podía escoger entre el archivo y tratamiento documental de la información por mecanismos manuales o tecnológicos. A partir de ésta época en mayor proporción el tratamiento se hace electromagnéticamente con aparatos y equipos informáticos y telemáticos, generando así una nueva cultura del tratamiento de la información producida por el derecho, pero a la par nuevos y variados riesgos, atentados y agresiones ilícitas públicas y privadas devenidos de esa tecnología. Los Estados, por su parte, como se ha dicho, han tomado

---

(22) Vid. Parte Tercera. La informática Jurídica y los datos de carácter personal. Ficheros o Bases de Datos.

una doble postura: una, preventiva, civilista y administrativa (*o de prima ratio)*; y otra, represiva (o *de ultima ratio)* previa la catalogación de tipos penales generales o específicos que tipifican Adelitos informáticos@ o hechos punibles en los que el fenómeno informático y telemático está presente como medio u objeto material de la comisión y/o ejecución del *iter criminis*, y en ambos casos, con excesiva Apunibilidad@, no totalmente justificada desde el punto de vista de una política criminológica de Estado frente a las nuevas tecnologías de la información y comunicación, como sucede en España [23], Australia [24], al crear tipos penales que atenta contra el derecho a la intimidad de las personas u otros bienes jurídicos como el patrimonio económico, la propiedad intelectual, etc. Igualmente, en el caso colombiano al agravar los tipos penales en los que se halle vinculada la tecnología informática o telemática, así se atente contra derechos fundamentales (la intimidad o el habeas data, honra, etc) o bienes jurídicos (patrimonio económico, fe pública, etc). Más adelante puntualizaremos sobre el tema.

4. LA CRIMINALIDAD CONCOMITANTE CON EL DESARROLLO TECNOLOGICO: EL HECHO PUNIBLE INFORMATICO.

4.1. En España, la legislación y doctrina mayoritaria no aceptan la existencia del delito informático. Por excepción, se acepta, teoriza y más aún , se clasifica.

4.1.1. Primera Postura: No existe el delito informático.

En Europa, a excepción de España, algunos Estados han regulado en sus códigos penales o leyes especiales, el denominado Adelito informático@, como veremos más adelante. En España, un gran sector de la doctrina iuspenalista, consideran incluso inadecuada hablar de la existencia

---

(23) En efecto, así se prevé como puntualizaremos más adelante (punto 5) y aunque la legislación y doctrina no reconoce la existencia tabulada en el C.P.de 1995, ni en ninguna otra ley especial de los llamados Adelitos informáticos@, pero sí la existencia de ilícitos penales en donde se utilizan medios comisivos informáticos o telemáticos o incluso en aquellos delitos que de alguna forma interviene un Aelemento informático@ y que atenta contra un bien jurídico definido como la Intimidad (Tit. X), el Honor (Tít. XI), o el APatrimonio y el orden socio-económico (Tit.XIII); entre otros. Una visión de precisa crítica al respecto se hace en el trabajo realizado sobre el título X del C.P.del 95, cuando se sostiene que Ala gravedad de las penas que se establecen para casi todos los supuestos puede llevar en algún caso a violar el ´principio de culpabilidad´, pues a la infracción cometida se fija una pena desproporcionada@. SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.*** En: Derecho Penal- Parte Especial. Ed. Dykinson, 2a, ed., Colaboración de Alfonso Serrano Mailló, Madrid, 1997. págs. 225 a 238.

(24) En Australia, sí se tipifica claramente los delitos informáticos en la ACrimes Act 1914" , como AComputer Crime@ En el AAct@, en las partes VIA (Arts. 76A a 76E y parte VIIB (Art. 85E,F), sobre delitos contra los datos o Ainformaciones personales@ a través de medios electromagnéticos, telemáticos y computacionales

como del nomen iuris de Adelito informático@, en el actual Código Penal de 1995, o en Leyes penales especiales o las extrapenales, como la LORTAD (Ley Orgánica No. 5, sobre la regulación del tratamiento automatizado de los datos de carácter personal de Octubre 29 de 1992), aunque esta última es de naturaleza iusadministrativa, la doctrina reconoce que esconde figuras delictivas.

Davara Rodríguez [25], con base en el principio penal universal de *nullum crimen, nulla poena, sine lege*, estima que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico protegido, ni que se haya determinado una pena para tales conductas, se puede concluir que no existe delito ni pena por las acciones tentadas o consumadas, por más dolosas que éstas sean.

Así mismo, deshecha el principio de la analogía de la teoría general del delito para aplicarlo a los llamados delitos informáticos, pues considera, el autor citado, que éste sólo será aplicable cuando beneficie a un Aencausado@, pero no para crear nuevos delitos, como se pretende por quienes quieren ver delitos informáticos tras haber incorporado el Código Penal del 95, figuras delictivas que atenta bienes jurídicos específicos como la Intimidad, el Honor, el Patrimonio y el orden socio-económico y que utilizan medios comisivos informáticos y telemáticos.

Sin embargo, el autor citado reconoce el impacto actual de las tecnologías de la información y la comunicación en la comisión de delitos, así como la necesidad de utilizar la nomenclatura de Adelitos informáticos@, para abarcar ese gran sector de la nueva criminalidad en los que se emplea a la informática o la teletransmisión de datos o informaciones como medios para cometer un delito, o para Aotras referencias a la informática y /o a la telemática, que figuran en el nuevo Código Penal@ Español de 1995, *por conveniencia, para referirnos a determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático* [26].

---

(25) DAVARA R., Ob. ut supra cit., pág.285-304. La posición de Davara es compartida por varios iuspenalistas como Valle Muñiz, Bueno Arús, Pérez Vallejo, Bustos Ramírez, Bajo Martínez; entre muchos otros.
(26) Ibídem pág. 304

Con aquéllas finalidades, *Davara* [27] define el delito informático como *la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*. En esta definición el autor sin quererlo aplica el concepto analógico del delito en términos generales previsto en la legislación española vigente y el vertido en las recomendaciones de la Organización para la Cooperación Económica y el Desarrollo Europeo (OCDE) [28]. Así mismo, incorpora no convenientemente en el mismo concepto, por un lado, todas aquellas acciones punitivas cuya comisión se realiza con medios o equipos informáticos, electromagnéticos, audio-visuales o de teletransmisión de datos; y por otra, las acciones punitivas que atenta derechos fundamentales, como la intimidad, la honra, etc., o bienes jurídicos tutelados por la ley, en los que se utiliza algún Aelemento informático@, bien sea logicial o de programas computacionales (software) o equipos físicos centrales o periféricos computacionales (hardware).

4.1.2. Segunda Postura: Posición ecléctica.

Sin embargo, *Pérez Vallejo* [29], recuerda que si bien no podemos hablar de delitos informáticos en la actualidad, la protección jurídica de la propiedad intelectual goza de raigambre en la legislación penal española desde el catálogo punitivo fundamental de 1848, aunque sostiene también, que por la aparición de nuevos los fenómenos tecnológicas ésta ha tenido que cambiar su regulación en la L.O. 10/95, para bien aunque parcialmente, puesto que se reprimen aquellas defraudaciones que centran su actividad principal en el acceso y manipulación de datos que se encuentran en soportes informáticos, o de programas de computador utilizados en su procesamiento.

---

(27) Ibídem pág. 288.

(28) La OCDE, 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). Delito informático, según la OCDE es: Acualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automatizado de datos y/o a la transmisión de datos@. Davara critica válidamente esta definición cuando sostiene que ésta no es muy técnica al apartarse del concepto mismo del delito y mencionar genéricamente a toda Aconducta ilegal@, cuando se puede tratar perfectamente de una acto tipificado en la legislación penal Ay el ordenador haber resultado accesorio por completo en la realización del mismo@.

(29) PEREZ VALLEJO, Ana. ***La informática y el derecho penal***. En: Actualidad Informática Aranzadi. A. I.A. Núm. 19 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996., pág.8 a 12.

4.1.3. Tercera Postura: El delito informático existe doctrinalmente.

Doctrinalmente se acepta la existencia del delito informático antes como después de la vigencia del Código Penal Español de 1995, tras analizar los contenidos normativos de otras latitudes como el ordenamiento jurídico-penal español.

En efecto, el profesor *Romeo Casabona* [30], estudia la posibilidad de estructurar un nuevo bien jurídico denominado de la Ainformación sobre la información@, como un bien que comporta por sí sólo un valor (económico, de empresa o ideal), relevante y digno de tutela jurídico-penal. Este valor será tan importante como para que la conducta humana sea calificada jurídicamente y pueda imponérsele una sanción correspondiente. Con base en esta estructuración, el autor citado siguiendo las clasificaciones de *Lamper y de Sieber* -- como lo afirma *Pérez Vallejo* [31]--, clasifica a los delitos informáticos en cuatros grupos o categorías. Clasificaciones que sirven a la citada autora, a *Gutiérrez Francés* [32] y *Buenos Arus* [33], para hacer su estudio sobre el delito informático en la legislación española antes de la vigencia del Código Penal de 1995 y con base en los anteproyectos y proyecto de Código Penal de 1992, pero a diferencia de todos ellos, el profesor Romeo Casabona, considera la información como valor no estrictamente ni sólo económico, sino que conlleve un valor relevante y digno de tutela jurídico penal.

Hoy por hoy, este derecho fundamental a la información o Aderecho a ser informado@, tiene su asidero en el art. 20.1 d), de la CE., y consiste en que toda persona tiene derecho no sólo para comunicar sino a Arecibir@ de las autoridades del Estado o las personas jurídicas públicas o privadas información concreta, oportuna y veraz dentro de los límites de la Constitución y el Ordenamiento Jurídico. No es simplemente la Aotra cara@ del derecho a comunicar la información, ni a emitir libremente sus ideas y opiniones, ya de palabra, ya por escrito, valiéndose de Prensa e

---

(30) ROMEO CASABONA, C.M., ***Poder informático y seguridad jurídica.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, ATendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías@, Madrid, 1993. Cit. Ob. Arus, pág. 2.

(31) PEREZ Valllejo. A. Ob cit., pág. 9.

(32) GUTIERREZ F., Mariluz. ***Notas sobre la delincuencia informática: atentados contra la Ainforma ción@ como valor económico de empresa***. En: Estudios de Derecho Penal Económico. Editores Luis A. Zapatero y Klaus Tiedemann. Ed. Univ. De Castilla-la Mancha, Tarancón (Cuenca), 1994. Pág. 183.

(33) ARUS B. F. Ob. cit ut supra. pág. 2 a 6.

Imprenta o de otro medio, sin sujeción a censura previa, como estaba previsto en las Constituciones Históricas Españolas, sino un derecho autónomo, complejo, dinámico, público y democrático según lo sostiene *Villaverde Menéndez* [34], por el cual, el Estado debe proteger a quien ocupa la posición de sujeto pasivo de la libre discusión de las ideas (opiniones e información) y a quien participa en él activamente como un emisor de las mismas; además, al receptor de esas ideas del propio emisor, el cual puede engañar o manipular a los receptores. No debe olvidarse que hoy en día por la universalización de los medios de comunicación social, el cúmulo de información que se emite y recibe es cada día mayor y los ciudadanos están expuesto en ese flujo constante de ida y venida de toda clase de información relevante y no únicamente aquella llamada con Avalor económico de empresa@. Por su parte el acceso a la información como derecho fundamental de toda persona, encuentra su fundamento constitucional en el art. 18 CE., cuando se reconoce genéricamente la limitación de la informática con relación a los derechos personalísimos de la intimidad, la propia imagen, el honor y el *pleno ejercicio de los derechos* fundamentales (STCS 254/1993 y Mayo 9/1994). Este derecho de acceso como el de actualización, rectificación y cancelación de la información se halla reglamentado en la LORTAD y Dec.1332/94, arts.12 y ss., principalmente.

Por su parte, *Carbonell y González,*[35] al estudiar el art. 197.2 del Código Penal Español del 95, lo intitula: *Los delitos informáticos*, para seguidamente expresar que éste numeral contiene a éstos delitos, Aaunque en puridad --dice-- se deberían llamar delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones@. Sin embargo, creemos los autores observan parcialmente el carácter por parte de la informática, que en éste caso es a la intimidad, pero no observan el de riesgo o inminencia atentatoria de un derecho fundamental o bien jurídico protegido fenómeno informático en forma holística, pues el misma art. 18 CE, sostiene el complejo asunto de los autolímites al ejercicio y potestad de los derechos fundamentales y en ellos

---

(34) VILLAVERDE MENENDEZ, Ignacio. ***Los Derechos del Público.*** Ed. Temis, Madrid, 1995, pág. 15 y ss.

(35) CARBONELL M. J.C. y GONZALEZ C.J.L., ***ADelitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.@*** En: Comentarios al Código Penal de 1995. Vol. I. Ed. Tirant lo blanch. Valencia, 1996, pág. 999

se menciona no sólo a la intimidad, la propia imagen sino al honor y *el pleno ejercicio de sus derechos* [36], con lo cual por defecto en el nomen iuris, podríamos entender por delitos informáticos, solamente a los delitos que atenta contra la intimidad. Súmese a ello, que en el C.P. del 95, existen otros derechos y bienes jurídicos llamados patrimoniales en los que la informática constituye ese potencial de riesgo e inminencia atentatoria que comentamos y que quedarían por fuera de la previsión planteada por los citados autores. En estas circunstancias el delito informático sólo contra la intimidad queda autodesvirtuado, al menos en el *nomen iuris*, en los términos de los autores citados.

Por contra, al derecho a la intimidad que subsume el de la propia imagen, el derecho al Ahonor@, no ha sido objeto de regulación jurídico penal en cuanto a los riesgos o atentados que supone la informática o telemática, en los términos del art. 18 de la CE. Sin embargo, la LORTAD, sí prevé infracciones y sanciones administrativas con el objeto de tutelar el honor contra atentados de las nuevas tecnologías de la información y comunicación. En la exposición de motivos de la ley, en el apartado séptimo (7), se precisa que *la Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento*, cuando en los arts. 42 y 43 las enuncia las infracciones graves, muy graves y leves.

4.1.4. Cuarta Postura: Clasificación del delito informático, en especial los que vulneran el derecho a la intimidad.

4.1.4.1. Clasificaciones guiadas por del derecho alemán. El bien jurídico tutelado: ALa información@.

Antes de la vigencia del Código Penal de 1995, *Gutiérrez Francés* [37], clasifica al delito informático, en tres grandes categorías, previamente a considerar la información con un valor estrictamente económico de empresa: A lo que tradicionalmente hubiera tenido una mera

---

(36) En concordancia con el art. 8 del Convenio Europeo de 1981 y los considerandos 2, 4,7, 9 y 10 de la Directiva 95/46/CE. STCS 254/1993 y de Mayo 9 de 1994.
(37) GUTIERREZ F., M. Ob. cit. pág. 184 a 208.

acumulación de datos, hoy, a causa del impacto de la revolución informática, se ha transformado en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico@. Sin embargo esa escisión tan cortante de la autora en la realidad no se presenta, valga el ejemplo de la conducta de los *hackers* (fusiladores o intrusos en los datos) sobre cualquier tipo de información. Esta conducta la realizan personas de cualquier edad, verdaderos adictos de la intromisión por placer o por desconocimiento o simple negligencia. Conducta diferente a la realizada por los *crackers* (rupturadores de datos), adictos delirantes que van sobre cualquier tipo de información con el objetivo de dañarla, inutilizarla total o parcialmente con diferentes métodos. Hackers y crackers van a por cualquier tipo de información o datos y no necesariamente los que denotan un Avalor económico@. Esto es lo que revela Ley Austriaca de 1987 de 22 de diciembre al tipificar el delito informático de ADestrucción de datos@ (126 a ostStGB) en el numeral 2, sostiene: *Se entiende por datos tanto los personales como los no personales y los programas.*

Las tres categorías de *Gutiérrez F.*, son: a) El espionaje informático industrial o comercial; b) Las conductas de daños o sabotaje informático que incluyen: la destrucción, modificación o inutilización de archivos y ficheros informatizados con valor económico de empresa; y, c) Las conductas de mero intrusismo, también conocidas por el término anglosajón *hacking.* Advierte, que las fronteras de estas divisiones no son categóricas, así como también que la dinámica comisiva de estos ilícitos pueden propiciar situaciones concursales. v.gr. Un comportamiento de espionaje empresarial puede ir acompañado de una modificación o destrucción de datos, subsumible en la categoría de sabotaje informático.

Posteriormente y en vigencia del C.P.del 95, *Pérez Vallejo* [38], siguiendo las clasificaciones de *Romeo Casabona*, agrupa a los delitos informáticos en cuatro bloques, a saber: a) Alteración de datos (Fraude informático), b) Destrucción de datos (sabotaje informático), c) Obtención y utilización ilícita de datos (espionaje informático o piratería de programas); y , d) Agresiones en el hardware (sustracción de servicios o hurto de tiempo). El término datos o información en la legislación alemana como

---

(38) PEREZ V. A. Ob cit., pág. 9 y ss.

comunitaria europea, son sinónimos.

Con esta presentación, la autora citada en vigencia del Código Penal del 95, estudia los delitos en los que tiene relevancia la informática para clasificarlos así: a) Delitos de carácter no patrimonial; b) Delitos contra el patrimonio; c) Delitos contra la propiedad intelectual; d) AOtras figuras delictivas@, y dentro de la cual involucra; entre otras, al Afraude informático@, trayendo a colación la Sentencia de 30 de Noviembre de 1988 de la Audiencia Territorial de Granada, refrendada por el Tribunal Supremo de 19 de Abril de 1991, sobre la interpretación flexible y teleológica de los tipos penales para dar solución a un caso en el que se utilizó un documento mercantil para cometer un delito de falsedad. El documento, objeto de la litis, no impreso o no tradicional --teniendo en cuenta la nueva definición del art. 26 del C.P., del 95-- lo aplicó a un Adocumento de la (sic) cinta o disco magnético acumulador o estabilizador de datos informatizados@.

En el primer grupo: ADelitos de carácter no patrimonial@, se ubican los delitos previstos en el Título X, del Código Penal Español, contra la AIntimidad, el derecho a la propia imagen y la inviolabilidad de domicilio@, en particular el Cap. I, ADel Descubrimiento y revelación de secretos, entra en una referencia directa a la informática@ el art. 197.2. No hace referencia a los delitos contra el honor, a pesar de citar el art. 18 CE., y ser éste otro de los importantes derechos de la personalidad considerado derecho Ano patrimonial@.

En el segundo grupo: ADelitos contra el patrimonio@, se relacionan los ADelitos contra el Patrimonio y contra el orden socio-económico@, en particular el Cap.II, sobre Alos robos@, el robo con fuerza y mediante Auso de llaves falsas@ (art. 238.4), es decir, las que enuncia el art.239 y resuelve de paso la controversia que se había presentado con el uso de tarjetas electromagnéticas, pues en la parte *in fine*, considera como llaves falsas Alas tarjetas, magnéticas o perforadas@. En el Cap. VI, ADe las defraudaciones@, Sec.I., art. 248.2, contempla la AEstafa informática@. En el Cap. IX, ADe los daños@, el art. 264.2, erige como delito el que Apor cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos@. Se establece así el delito contra el equipo computacional físico o los sistemas y programas lógicos (hardware y software).

En el tercer grupo: *Delitos contra la propiedad Intelectual*, relaciona el Cap.IX: *Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores* (Tít. XIII, ADelitos contra el patrimonio y contra el orden económico-social@ C.P.del 95). En la Secc. 1, *De los delitos contra la propiedad intelectual* tipifica algunas conductas en atención a la incidencia actual de las nuevas tecnologías de la información y la comunicación ocasionadas en la obras de creación o intelectuales.

Sobre éste punto es destacar que el C.P., vigente nada nuevo destacable introduce a lo preceptuado en el anterior Código Penal Español., en los arts. 534 bis a) a 534 ter.

4.1.4.2. Clasificaciones del delito informático en donde uno de los bienes jurídicos a proteger más importante es la *Intimidad*.

Sin embargo, es de destacar en el derecho penal español la cuidadosa como compleja redacción de normas que tipifican delitos contra la intimidad y la propia imagen (no así el honor), como derechos fundamentales altamente protegidos en los art. 18.4, 20.1.d) y 105 CE, contra las injerencias de la informática.

El iuspenalista español *Morales Prats* [39], quien se ha preocupado desde su tesis doctoral en 1983, por el estudio del derecho a la intimidad, la informática y el derecho penal, hace un detallado estudio actual y retrospectivo de éste complejo derecho fundamental a la luz de las tecnologías de la información y la comunicación.

En efecto, el autor analiza el Título X, *De los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio* (arts. 197 a 204) del C.P., del 95, y considera que la *privacy*, Alibertad informática (faceta o perfil informático de la intimidad)@, en el art. 197.2, tipifica un elenco de conductas que comportan Aabusos informáticos@, aunque no en forma completa, pero sí más coherente en la descripción de conductas típicas codificadas y en forma cerrada. No es completa, porque el art. 197.1, recoge las conductas de interceptación, grabación o

---

(39) MORALES PRATS, F. Ob. ut supra cit., págs. 299 a 322.

reproducción electrónica ilícita de comunicaciones informáticas (mensajes de correo electrónico). Igual la captación subrepticia de mensajes de correspondencia electrónica y el apoderamiento físico subrepticio, con la intención de descubrir la intimidad ajena de mensajes de correspondencia informática ya impresos fuera del sistema.

Es coherente, porque finalmente el art.197.2, en su redacción es sustancialmente mejor que la presentada en el proyecto de Código Penal de 1992 (art.198.2) y del proyecto de C.P. de 1994 (art.188.2), textos en los que se tipificaba únicamente el apoderamiento no autorizado de datos personales.

El mentado artículo es una norma cerrada, pues antes que la técnica de tipi- ficación de conductas de ley penal en blanco se escogió la de la codificación y describir las conductas delictivas en forma cerrada para incriminar los delitos contra el *habeas data* o *libertad informática*. Técnica que suscita problemas a la hora de esclarecer las conductas y evidente incorrección en la definición técnica de las conductas típicas, pues para ello hay que recurrir a la LORTAD y otras normas extrapenales que informan las conductas penales previstas en el art. 197.2., como el Convenio de 28 de Enero de 1981 del Consejo de Europa y la Directiva 95/45/CE, del Parlamento y el Consejo de Europa, que completa y amplia la protección del Convenio sobre las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Las conductas típicas previstas en el art. 197.2. CP.del 95, --dice el citado autor- son: a) En el inciso primero, quedan tipificadas las acciones de apoderamiento, utilización o modificación de datos reservados de carácter personal, que se hallen automatizados de forma electrónica o que obren en cualquier otro tipo de archivo o registro público o privado. Estas acciones deben realizarse *sin autorización* y *en perjuicio de tercero*; b) En inciso segundo, se tipifica la acción de acceder por cualquier medio a los datos personales y a quien los altere o utilice en perjuicio del titular o de un tercero.

Los tipos penales básicos podrán presentarse como agravados, siempre y cuando se tipifiquen las siguientes conductas:

a) Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas. Este es un tipo penal compuesto (estructura típica doble), que requiere la previa comisión de uno de los tipos penales básicos del art. 197.1 y 197. 2 (apoderamiento de documentos electrónicos , al de control audio-visual telemático en forma clandestina y los relativos a los abusos informáticos contra el habeas data), según fuere el caso y previsto en el art. 197.3., como un tipo agravado de revelación, difusión o cesión a terceros de datos, hechos o imágenes;

b) Si se realizan por determinadas personas. Es el tipo agravado en razón a la esfera de dominio profesional del sujeto activo, según el art. 197.4, es decir, que tengan la condición de encargados o responsables de los bancos de datos (o *ficheros*), soportes informáticos, electrónicos o telemáticos, archivos y registros;

c) Si se revelan datos de carácter personal específicos. Es el Tipo agravado en razón de la afectación del *núcleo duro de la privacy*, es decir, contra los datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, según la primera parte del art.197.5;

d) Si la *víctima* fuere especial por su edad y/o aspecto sensorial. Es el Tipo agravado en razón de que la víctima sea un menor o incapaz, según la parte *in fine* del art. 197.5.

Estos dos tipos agravados (c y d), obedecen a una sana como acertada política criminológica de los Estados al proteger la esfera más íntima de la intimidad, no informatizables según las normas internacionales y recomendaciones europeas (Convenio de 1981 y Directiva 95/46/CE) y de reforzarla en el caso de los menores y personas con minusvalía.

e) Si se realizan contra el *núcleo duro* de la intimidad. Es el Tipo agravado en consideración a los fines de lucro perseguidos, según el art. 197.6 C.P, si conlleva la realización de los tipos anteriores (1 a 4 del art. 197). Si además, se realiza en atención a la conducta prevista en el art. 197.5, contra el *núcleo duro de la privacy*, se impone una *Apena hiperagravada de cuatro a siete años de prisión@*, como lo puntualiza el *Morales Prats* [40].

(40) Id. pág. 321.

f) Si la autoridad o funcionario público realizara una *cualquiera de las conductas descritas en el artículo anterior* (197 CP. Se entiende entonces que no hay exclusión de ninguna modalidad delictiva), fuera de los casos previstos en la ley, sin que medie causa o investigación judicial por delito, y *prevaliéndose del cargo*. Es un tipo agravado en razón de la calidad del sujeto activo, prevista en el art. 198 C.P., y por tanto, con penas más severas. A esta norma se le han hecho varias críticas que las resumimos así: 1. Se considera innecesaria, pues hubiese sido suficiente con la aplicación de la agravante séptima del art. 22 del C.P.[41], sobre la prevalencia del carácter público que tenga el culpable; 2. Hacer referencia a cometer el hecho fuera de los casos previstos en la ley *Aes meramente residual, pues se refiere a la falta de concurrencia de una causa de justificación@*[42] ; y, 3. Además de los *Adefectos de coordinación sistemática* planteados por *Morales Prats@*[43], respecto del art. 198 y los arts. 535 y 356, sobre los delitos cometidos por funcionarios públicos contra la intimidad y siempre que haya mediado causa por delito, es evidente que las normas constituyen las dos caras de la transgresión a la intimidad por un funcionario público: con o sin causa por delito, pero con diferente graduación punitiva lo cual supone la aplicación del principio de favorabilidad sobre las penas a imponer.

4.2. En Colombia. No existe el delito informático en la legislación, pero sí tipos delictivos en los que está presente la informática.

4.2.1. Tesis Negativa: *nullum crimen sine lege previa penale.*

Actualmente no existe el delito informático como tal, ni en el Código Penal, ni en la legislación especial, básicamente por las mismas razones dadas en el derecho penal español y por otras particulares expuestas por la doctrina colombiana.

En efecto, abundando en la tesis negativa a la existencia del delito informático *Rivera*

---

(41) SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad...*** pág. 235

(42) AA.VV. ***Código penal. Doctrina y jurisprudencia.*** Tomo II, Artículos 138 a 385. Dirección: Cándido Conde-Pumpido F., Ed. Trivium, S.A., 1a ed., Madrid, 1997. págs.2329 y ss.

(43) MORALES PRATS, F. Ob.ut supra cit., pág. 325

Llano [44], considera que al no estar tipificados la legislación vigente, éstos no existen. Lo que sí existe --dice-- son conductas no éticas y antijurídicas cuyos medios de ejecución se verifican con medios modernos o tecnológicos y, por tanto, la valoración de los mismos es nula ya que las conductas son asimilables o están tipificadas en los actuales Códigos Penales. Claro está que estas argumentaciones se quedan sin demostración, pues no se analiza cuáles, cómo y de qué forma se asimilarían los tipos penales actuales al denominado delito informático, a fin de que no sea necesaria su estructuración típica y autonómica.

4.2.2. Tesis Ecléctica: Las nuevas tecnologías de la información imponen una tutela penal.

Rivera Llano [45], a pesar de negar la existencia del delito informático, reconoce que los avances de las tecnologías de la información, han ocasionado una especie de *segunda revolución: la informática*, y como tal, los Estados deben afrontar esta situación tutelando penalmente las agresiones que se cometan contra la información. *La era de la información*, está marcada por el desarrollo constante de la industria y la tecnología de la telecomunicación, la miniaturización de los *chips*, la globalización del uso de computadores para toda clase de servicios desde los empresariales hasta los meramente familiares y personales. *AEsta marcha triunfal de las aplicaciones de la informatica no solo tiene un lado ventajoso sino plantea tambien problemas de importancia crucial para el funcionamiento y la seguridad de los sistemas informaticos en el mundo de los negocios, la administracion y la sociedad en general@*; y por ello, para paliar algunos de estos problemas debe erigirse el delito informático (*computer crime*) para proteger los atentados de la *criminalidad informática* que cada día crece en el mundo, teniendo como bien jurídico protegible el de *la información*.

El autor citado, siguiendo en términos muy generales la clasificación de *Ulrich Sieber*, en cuanto a la información creada, procesada o recuperada por medios compu-

---

(44) RIVERA LLANO, Abelardo. ***Dimensiones de la informática en el derecho***. Ed. Jurídica Radar, Santa fe de Bogotá, 1995, pág. 89 y ss.
(45) Ibídem pág. 89 y ss.

tacionales, informáticos o telemáticos y luego de aceptar doctrinalmente la existencia de los delitos informáticos, expone que en éstos lo principal no son los medios tecnológicos empleados en la comisión del delito sino el objeto material contra el que van dirigidos, es decir, la información (en su *creación , destrucción o uso*) procesada por la tecnología.

En tal virtud, clasifica a los delitos informáticos, a saber: a) Delitos contra la información por creación, b) Delitos contra la información destrucción total o parcial, c) Delitos contra la información por uso indebido, inapropiado o no autorizado, d) Delitos contra la información por medio de sustracción, que se puede concretar por la simple obtención en A*pantalla*@ o por copia de programas o archivos.

En esta concepción y clasificación del delito informático predomina como característica la de considerar a la *información*, en general (electromagnética, computacional o telemática) como bien jurídico tutelable por el Estado. En dicho bien se subsumen derechos no patrimoniales y patrimoniales que otras legislaciones como la española identifican autónomamente, como antes se analizó.

4.2.3. Tesis positiva: El delito informático como producto concomitante de las nuevas tecnologías de la información y comunicación. Técnica Penal similatoria de tipos.

Por su parte, el Criminólogo *Molina Arrubla* [46], al hablar de las diversas formas de la criminalidad actual, las clasifica así: a) Por la Estadística, b) Por sus Agentes, c) Por su ámbito; y d) Por su Desarrollo. Dentro de éste último grupo, incluye: a) La *Criminalidad Retrógrada*, es decir, la referida al pasado, ubicando entre ellos los *delitos de Sangre*; b) La *Criminalidad Anterógrada*, es decir, la criminalidad que tiende a generalizarse hacia el futuro, como son las delincuencias en el campo internacional y transnacional; y c) La *Criminalidad evolutiva*, es decir, aquella que nace concomitantemente con los avances tecnológicos, mercantiles, industriales y con métodos sofisticados y perfeccionistas utilizados en la comisión de los ilícitos. La

---

(46) MOLINA A. Carlos. ***Introducción a la criminología***. Ed. Biblioteca Jurídica, Medellín, 1988, pág. 305 y ss.

comisión y ejecución de estos hechos se hace por regla general, a través de labores de inteligencia, como sucede en los fraudes y quiebras simuladas. En otras ocasiones dan origen a una nueva vertiente de la criminología que se conjuga en el llamado *Delito Económico*, o en su caso, por el avance de las nuevas tecnologías de la información y comunicación.

En consecuencia, los A*delitos de informática*@, son producto de la criminalidad evolutiva, la cual nace concomitantemente con las nuevas tecnologías informáticas y telemáticas y el *delito informático* es aquél se comete con el empleo de computadores o equipos electromagnéticos que transmiten datos o *informaciones*.

Los delitos informáticos, según *Tiedemann*,

> *alude (n) a todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de datos. Por una parte, dicho concepto abarca pues el problema de la amenaza, asociación y divulgación de datos obtenidos por computadores..., y por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el abuso de datos procesados automáticamente...* [47] .

Esta definición contempla el concepto de delito informático con base en los problemas sobrevenidos en el proceso de tratamiento automatizado o computacional de la información personal o los datos de carácter personal, desde aquellos en los que se utiliza como medio comisivo a los equipos electromagnéticos para procesar información hasta aquéllos en los que la recolección, utilización, recuperación y abusos de la información constituyen el objeto material del ilícito e igualmente la información con bien jurídico protegible.

Molina A., siguiendo a *Tiedemann* [48] , profesor del Instituto de Criminología y Derecho Penal de Friburgo (Alemania), clasifica a los delitos informáticos así: a) Las Manipulaciones que una persona realice en las actividades de entrada y salida de información o de datos computarizados; b) El Espionaje económico, teniendo en cuenta
que la información se almacena en soportes electromagnéticos, la transferencia de datos de un lugar a otro por cualquier medio sistematizado es lo más usual actualmente. Este

---

(47) TIEDEMANN, K., citado por Molina A. ob. ut supra., pág. 307
(48) Ibídem.

espionaje económico se utiliza por empresas rivales, así como con finalidades políticas por Estados Extranjeros; c) Sabotaje. Se produje daño, destrucción, inutilización en el procesamiento de datos o información automatizada, en programas o software total o parcialmente; y, d) Hurto de tiempo. Tiene cabida en la indebida utilización, sin autorización de equipos computacionales o salas informáticas. Se penaliza el uso indebido y el tiempo de procesamiento de información o de datos perdido por el propietario con las inapropiadas actividades.

El autor citado, al aplicar esta clasificación del delito informático alemana al caso colombiano, comienza diciendo que el bien jurídico tutelado en estos casos prioritariamente es el *Patrimonio Económico* (Título XIV del C.P.Col.), con lo cual no descarta otros bienes tutelables, ya que considera que la mayoría de las conductas delictivas que se cometen con computadores oscilan entre el hurto, la estafa, el fraude, el abuso de confianza y el daño. Esta técnica asimiladora es una postura tradicional que no aporta mucho a la tesis positiva del delito informático, sino al contrario trata de desvirtuarlo, pues se estima que no hay necesidad de darle autonomía jurídica, ya que basta con estudiar el fenómeno de las nuevas tecnologías de la información y comunicación a la luz de los tipos actualmente existentes en el Código Penal y adecuarlos normativamente, si fuere del caso, o adicionarlo a los tipos existentes como causales de agravación punitiva. Sin embargo, al encasillar los actuales tipos penales previstos en el C.P., en la clasificación alemana está reconociendo la existencia del delito informático, no sólo en la doctrina sino en la legislación penal vigente, y por ende, la necesidad de tipificarlo y darle autonomía propia y un bien jurídico tutelable. Quizá sólo por ello, la técnica que llamamos asimiladora de tipos penales es el primer gran paso a la autonomía del tipo penal informático en el derecho colombiano.

Al tratar de encuadrar el *Hurto de Software y espionaje*, el citado autor no tuvo en cuenta la abundante legislación existente sobre el tema, aparte de la que fue objeto de su estudio (Código Penal: *Delitos contra la propiedad*, Tit. XIV y *Delitos contra el orden económico social*, Tit. VII). En efecto, se dejó de lado toda las normas penales especiales previstas en la regulación sobre propiedad intelectual y a la protección de los programas computacionales o *software*, como una de sus especies (Ley 23 de 1982 y 44 de 1994), la prevista en la Ley 296 de 1996, sobre Libertad de competencia económica e infracciones a la

misma y las Decisiones 351/93 y 344/94 del Parlamento Andino, sobre propiedad intelectual e industrial, respectivamente.

En las anteriores leyes se prevén tipos penales y contravencionales específicos que protegen la propiedad intelectual, y en especial, el software contra atentados de copia, procesamiento, apropiación, uso indebido, etc., pues el software es un trabajo intelectual de "pensamiento-resultado" [49] , A*la expresión de un conjunto organizado de instrucciones, en lenguaje natural o codificado, independiente del medio en que se encuentre almacenado, cuyo fin es el de hacer que máquina capaz de procesar información, indique, realice u obtenga una función, una tarea o un resultado específico*" (art. 3, lit., a Dec.1360/89), que justifica la protección jurisdiccional.

4.2.4. Tipos delictivos en los que está presente actualmente el fenómeno informático. Bien jurídico: A*Habeas Data@.*

Hemos sostenido antes que la informática y/o la telemática puede afectar a bienes jurídicos patrimoniales y no patrimoniales, como también, a derechos fundamentales y libertades constitucionales, como la intimidad y el *habeas data*. Los diferentes tipos están previstos en los Códigos Penal y Nacional de Policía, y en los estatutos penales especiales v.gr. los que regulan *la propiedad intelectual* [50] y la *propiedad industrial*. Las normas extrapenales (códigos civil, mercantil y administrativa, principalmente), brindan una protección jurisdiccional preventiva, interpretativa y hermenéutica a la punitiva, pero prioritariamente a la propiedad intelectual e industrial.

En estos estatutos penales principales, especiales y complementarios encontramos

---

(49) Sentencia T-80, Feb. 26/93. Corte Constitucional, Sala II., Rev. M.P. Eduardo Cifuentes. En: AA.VV. ***Base de Datos Legis.*** Ed. Legis. Santa fe de Bogotá (Col), pág.44-7**.**

(50) Legislación de Derechos de Autor o propiedad intelectual en Colombia, ha recogido mediante la incorpo ración legislativa al derecho interno, los diversos Convenio Universales que sobre el asunto se ha suscrito. En efecto, mediante la Ley 46 de 179, los mecanismos de protección al derecho autoral previstos por la OMPI en Estocolmo de 14 de Julio de 1967. Mediante Ley 23 de 1992, el Convenio de Ginebra para la protección de fonogramas contra la reproducción no autorizada; El tratado de Ginebra sobre registro internacional de obras audiovisuales, mediante Ley 26 de 1992; El Convenio de Berna para la protección de obras literarias y artísticas, por Dec. 1042 de 1994 y la Decisión 351 del Pacto Andino, sobre propiedad intelectual. Las leyes 23 de 1982 y 44 de 1993, constituyen el marco normativo fundamental para la protección civil y penal de la propiedad intelectual en Colombia. Por lo que respecta al hecho punible (Delitos y Contravenciones) contra este derecho fundamental y de contenido omnicomprensivo, se regula en los arts. 30 y ss y arts.232 a 257, de las leyes citadas. En particular, sobre la protección al sofware, se estableció penas principales y accesorias severas que van desde la prisión y multas por la copia ilegal, la apropiación o el uso indebido de programas de computador hasta la incautación y destrucción de los productos informáticos obtenidos irregularmente por parte de la policía judicial.

hechos punibles que la doctrina universal califica de informáticos, ya sea por que en su comisión se utilizan medios u objetos electromagnéticos: informáticos y/o telemáticos, o porque el derecho de acceso a la información o *habeas data*, constituye un bien jurídico tutelable por el Estado. Algunos de estos tipos punitivos (delitos y contravenciones) se han relacionado antes [51]. En éste aparte relacionaremos otros más.

Un aspecto capital a destacar de las diversas posturas doctrinales mencionadas es el planteamiento del bien jurídico del derecho fundamental de @*Habeas Data*@ cuya tutela o garantía estatal puede válidamente sostenerse en el derecho penal colombiano, entre otras razones, por las siguientes:

En Colombia, se ha constitucionalizado el derecho de *habeas data,* o sea, derecho que tiene toda persona a acceder a la información relevante que le compete, así como a conocerla y solicitar, si fuere del caso, la actualización y la rectificación de la misma (art. 15 Constitución Colombiana), tanto de la información obtenida o procesada mecánicamente (oral, escriturario o impresa), como la que ha sido objeto de procedimientos automatizados por equipos computacionales, informáticos o telemáticos y se ha almacenado en dispositivos electromagnéticos (discos fijos, removibles, CD-ROM y RAM o DVD o Disco Digital de Video) [52], en bancos de datos de carácter público o privado. Este derecho de acceso a la información se extiende también al derecho que tiene toda persona a demandar de cualquier autoridad estatal el Aacceso a los documentos públicos salvo los casos que establezca la ley@ (art. 74 Cons.Col), es decir, el C.C.A., y la Ley 57/85, principalmente.

Igualmente para interpretar el ámbito, alcance y limitaciones del derecho de acceso a la información se deberá estudiar la vertientes que tiene el derecho a la información (art. 20) como derecho fundamental de toda persona en los términos que la legislación universal lo ha instituido (Art. 19 de la Declaración universal de Derechos Humanos de 1948) y que la Constitución de 1991, ha elevado a rango constitucional el derecho de toda persona a A*informar y recibir información veraz e imparcial*@ (arts. 20), como derecho genérico y la libertad de expresión o

---

(51) Véase, apartado 2.2., de ésta Parte

(52) A Y hoy, cuando casi se cumplen dos décadas del disco compacto, una nueva tecnología ha hecho su aparición, el DVD (Disco Digital Versátil), que supera en siete veces la capacidad de almacenamiento de su predecesor@. Vid. Diario EL MUNDO, Domingo 5 de abril de 1998, págs. 12 y 13. Igualmente, Mi trabajo ***La Constitución...*** ob. cit. págs.127 a 224.

A*prensa*@ (art. 73) y el derecho de toda persona de acceder a los documentos públicos, salvo las excepciones de ley (art.74), como derechos igualmente fundamentales específicos. En efecto, en el derecho constitucional colombiano, el derecho a la información no sólo se extiende a la vieja libertad clásica e individualista de la *libertad de prensa* vista de un aspecto simplemente activo, es decir, desde el emisor o productor de la información sino también del receptor o consumidor de la información.

La Constitución colombiana, al igual que lo hiciera la Brasileña de 1988 y mucho antes la Portuguesa de 1976, constitucionalizaron el llamado A*Habeas Data*@, con diferente técnica y efectos, pero las tres elevan a rango constitucional lo que se ha conocido como *informática* , el derecho fundamental de habeas Data, y en forma particular, la Constitución Colombiana, constitucionaliza las fases del tratamiento automatizado de datos y los límites y autolímites que debe observar con respecto a los demás derechos y libertades constitucionales. En consecuencia, el art. 15 de la Constitución Colombiana, siguiendo los pasos de la Constitución Portuguesa (art. 35) y Brasileña, incorporó el *Habeas Data* en el texto constitucional, no como un derecho autónomo como en aquéllas Cartas, sino como un derecho contenido en otro gran derecho continente que tutela A*la intimidad personal y familiar y el buen nombre*@. Técnica esta última que se presta a muchas interpretaciones, entre otras, como la seguida en el derecho constitucional español cuando la doctrina ha escindido de un mismo texto constitucional, otros derechos autónomos o Aderechos constitucionales nuevos@, con igual rango del que nació, tal como se viene sosteniendo tras el planteamiento del iusfilósofo *Pérez Luño*, [5 3] con la llamada A*Libertad informática*@, escindida del art. 18.4 CE., que regula la informática como límite al ejercicio los derechos fundamen- tales, como la intimidad, honor, imagen, etc., ampliamente criticada en la Parte II.

Otra interpretación diferente es la que se dio por parte del constituyente colombiano en la Constitución de 1991, al incorporar antitécnicamente en un mismo artículo tanto el derecho constitucional de *habeas data* como los derecho el fundamental de la intimidad (que subsume el llamado del Abuen nombre@o de la Apropia imagen@),

---

(53) PEREZ LUÑO, Antonio Enrique. ***Derechos humanos, estado de derecho y constitucional.*** Ed. Tecnos, Madrid, 1984. págs.359 y ss.

pero el primero (*habeas data*) en forma expresa y demasiado amplia que más parece un texto de rango legislativo que constitucional. En efecto, se define el habeas data, el procedimiento de recolección y tratamiento de la información mecánica y/o informática, las excepciones en la comunicación privada, las interceptaciones judiciales a la comunicación, así como la extensión a documentos específicos, como los tributarios, por ejemplo. Allí mismo iniciando el artículo se constitucionaliza el derecho a la intimidad personal y familiar, como derecho fundamental objeto de protección especial por parte del estado. Los dos derechos están completamente individualizados, pero el constituyente los fusionó como si se tratara de un mismo fenómeno jurídico, o en consideración media, como si se tratase de derechos complementarios e inseparables y esto no es del todo así. Esta técnica del Constituyente colombiano ha sido objeto de crítica en la Parte II.

La Corte Constitucional Colombiana, paulatinamente va desentrañando la autonomía del derecho de *habeas data* y la intimidad, como hemos visto en la Parte I y II de esta investigación, [54] basados en lo que les da identidad y separabilidad: por un lado, los valores constitucionales como la dignidad y el respeto de la persona humana, y la conexión con el derecho de autonomía personal; y por otro, los límites a las demás libertades y derechos fundamentales, como el derecho a la información , el acceso a los documentos públicos o privados, entre otros. Y es, precisamente en la teoría de los límites y autolímites a los derechos constitucionales donde aflora la separabilidad de uno y otro derechos, pues se ha encontrado que una de las mayores vertientes a los A*abusos de la información*@ han dado origen a A*un nuevo derecho denominado habeas data*@[55] en el derecho constitucional colombiano.

Concordantemente, hemos sostenido que con la manipulación de la información mecánica (impresa) o automatizada (informática), no sólo se vulnera derechos patrimoniales y no patrimoniales sino también derechos de tratamiento jurídico *sui géneris*, como el de la propiedad intelectual o la industrial. En tal virtud, no podemos simplemente supeditar *el habeas data* a la intimidad, ni menos fusionar el uno al otro, como si fuese uno

---

(54) Vid. Corte Constitucional: Sent. T-414, Jun. 16 de 1992. M.P. Ciro Angarita; Sent. T-512, Sep.9 de 1992. M.P.José Gregorio Hernández; y, Sent. T-022, Ene. 29 de 1993, M.P.Ciro Angarita. En: AA.VV ***Base de Datos Legis.*** Ed. Legis. Santafé de Bogotá (Col), pág.44-6 y ss.

(55) Vid. Corte Constitucional: Sent. C-114, Marz.25 de 1993. Sala Plena. Ob.cit. pág. 428.

solo [56] y como sí el derecho de *habeas data* sólo afectara al derecho de la intimidad y no al cúmulo de derechos y libertades públicas, y además porque, un sector de la doctrina iusinformática ha planteado sus diferencias de contenido, alcance socio-jurídico y carácter proteccionista por parte del Estado [57].

Esta técnica *sui géneris* de codificación constitucional conduce a diversas como erróneas interpretaciones por parte del operador jurídico, por ejemplo, la de entender que el derecho de *habeas data* sólo afecta al derecho de la intimidad y no a ninguno otro derecho personal y/o patrimonial --como es la tendencia generalizada--, por la exclusión formal de los demás derechos o libertades en los que éste no está incluido.

Por contra, creemos que una recta interpretación de la norma nos debe conducir a entender que dicho texto afecta al cúmulo de derechos y libertades constitucionales que se hallan previstas en la Constitución y no solamente a los previstos en el título II, *De los derechos, las garantías y deberes*, como fundamentales , pues aquéllos se reputan no por su mera ubicación formal en la Constitución, ni por ser de aplicación inmediata (art. 85 Cons.Col), o ser objeto de A*Acción de Tutela*@ (art. 86 id), sino por su contexto, forma y ámbito de injerencia como derecho en la dignidad y respeto de la persona humana, o por criterios principales y subsidiarios no concurrentes determinados por el juez de tutela [58].

---

(56) Tal como lo analiza Londoño, el iusfilósofo Frosini V. en su obra A ***La protección de la intimidad: De la libertad informática, al bien jurídico informático@***, considera el derecho de habeas data como una extensión del derecho a la intimidad o del Aright to privacy@, pero con un contenido actual más acorde con la realidad. La autora se refiere, a la concepción del Ahabeas data como aquél derecho que surge fruto de la tecnología informática y que 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@. En ésta última visión se desconoce el concepto de habeas data por procesos diferentes a los automatizados. ***Informática jurídica y derecho informático.*** Ed. Señal, s/n, Medellín (Col), pág. 33 y ss.

(57) Por el contenido, se tiene la dificultad para delimitar el verdadero contenido de la intimidad, por contra al del habas data que tiene un carácter objetivo en su definición ("la libertad reside en la habilidad para controlar el uso que de esos datos personales se haga en un programa de computador" y de contenido Amuy amplio@, es el derecho al acceso de los bancos de datos, el derecho a verificar su exactitud, el derecho a verificar su exactitud, el derecho a actualizarlos y a corregirlos, el derecho a mantener en secreto a los datos sensibles, el derecho a ningún pronunciamiento acerca de los llamados ´datos sensibles´ A). ALa teoria tradicional de los derechos humanos solo hace referencia a su exigencia frente al Estado, y aunque el derecho a la intimidad generalmente se ha hecho valer por un particular frente a otros particulares, el Habeas Data ha aumentado su alcance... EI Habeas Data es un derecho humano que en su moderna tendencia coloca a los particulares con una responsabilidad muy clara frente al respeto de estos derechos. Todo lo anterior no nos autoriza --sostiene-- sin embargo a negar que la garantia de proteccion del Habeas Data pertenece y se hace exigible a través del Estado@. Ob. cit. pág. 33 y ss.

(58) Sent. T-002, Mayo 8 de 1992, Corte Constitucional. M.P.: Alejandro Martínez C., En: AA.VV. ***Base de Datos Legis.*** Ed. Legis. Santa fe de Bogotá (Col), pág. 722.

Ahora bien, los hechos punibles (delitos y contravenciones) en los que está presente el fenómeno tecnológico de la información y la comunicación: informática y/o telemática, están actualmente ubicados en el Código Penal de 1980 y el Código Nacional de Policía, en las leyes punitivas especiales como la que protege la propiedad intelectual e industrial, bajo diferentes bienes jurídicos, ubicación y dosimetría penal.

I.- ***Delitos previstos en el Código Penal del 80, a saber*:**

A. *Delitos de los datos o informaciones automatizadas contra un bien jurídico tutelado:*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.

B. *Delitos contra los datos o informaciones automatizadas que se hallan bajo diferentes bienes jurídicos*: 1) *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).

2) *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).

La legislación extrapenal amplía la gama de protección: El Código del Comercio reformado parcialmente por la Ley 256 de 1996, sobre protección a la libertad de competencia económica, prevé un proceso civil abreviado contra actividades que implican competencia desleal y violación de secretos (artículos 16 a 33). Igualmente en otras normas sobre marcas y patentes (artículos 583 y ss., del C.de Comercio); y, finalmente en la Decisión 344 de 1992, sobre propiedad industrial del Pacto Andino.

3) *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*@ [59] . 3. Daño agravado cuando se comete en A*archivos*@ (se entiende

---

(59) VALLE MUÑIZ, José M. Ob. ut cit. pág. 489

manuales o informatizados), art. 371.4.

4) *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.) dentro de los cuales se incluyen los atentados producidos por la informática y/o telemática contra éste derecho fundamental, subjetivo e intangible [60] v.gr. accesos, procesamientos y abusos informáticos y la denominada A*piratería*@: electrónica y material del software. A*Se castiga* (la fabricación, puesta en circulación y) *la tenencia o introducción en el mercado* (clandestino) *de los medios de inutilización* (o neutralización), *con independencia de que se hayan usado o no*@ [61] , tal es el caso de los programas virus o desencriptadores o inutilizadores de *password*.

II.- *Contravenciones de los datos o informaciones automatizadas contra un bien jurídico tutelado.* En el Código Nacional de Policía, (C.N.P.) se prevé las contravenciones especiales que A*afectan la integridad personal*@, la intimidad o la A *vida íntima o privada de una persona*@ (arts.46 a 49), cuando sin facultad legal se la averigüe hechos o datos de la intimidad, se los graba con cualquier medio tecnológico de información o comunicación que llama A*subrepticios*@, o los A*divulga*@ u obtiene A*provecho*@ de ese descubrimiento de información. Estas modalidades ilícitas se agravan si se hace a sabiendas, con conocimiento previo y sin justa causa.

El C.N.P. desde 1970, a diferencia del C.P.Col y chileno [62], expresamente estipula el _____

(60) Sent. 1617 de dic. 14 de 1990. Sala Contencioso Administrativo. Sec. I. M. P.: Dr. Rodrigo Viera P.

(61) QUINTERO OLIVARES, Gonzalo. Ob. ut supra cit. pág.572. Los paréntesis son nuestros.

(62) En el Código Penal chileno se estructura un tipo delictivo específico pluridefensivo con acciones múltiples dirigidas a proteger el derecho de la información. Aunque el tipo adolece de un técnica político-penal, soluciona de otra parte, los innumerables problemas que se presentan con el proceso automatizado de la información desde la fase de recolección (Ainput@), pasando por la fase de procesamiento propiamente dicho (Ain@), hasta llegar a la fase de recuperación o salida de información (Aoutput@). Este tipo penal subsume por tanto, las figuras delictivas previstas en la clasificación de *Tiedemman y Molina A,*. En efecto, se prevé "el acceso indebido, el apoderamiento, la destrucción, inutilización, transformación o desfiguración de una información con el fin de impedir u obstaculizar su procesamiento automático o de revelarla o transmitirla indebidamente", además como lo sostiene *Correa*, desde el proyecto de la nueva figura delictiva se propuso agravar la pena de los demás delitos cuando éstos sean cometidos por medios informáticos. Vid. CORREA, C. *Informática y derecho*. Ed. Depalma, Buenos Aires, 1988, pág.24

derecho a la intimidad de las personas como bien jurídico protegido contra agresiones que utilicen cualquier medio subrepticio (incluidos los informáticos) y persigan desvelar furtiva o ilegalmente hechos, actos o datos de la vida privada. Este código de 1970, ya preveía una modalidad de hecho punible (contravención) contra la intimidad, y quizá por ello el C.P.Col., en 1980, se abstuvo aparentemente de proteger penalmente este bien jurídico específico en forma expresa y prefirió tutelar el descubrimiento de datos, hechos o actos de la vida privada o íntima tácitamente bajo el bien jurídico de *Libertad Individual y otras garantías*, como antes comentábamos [63], quizá para ampliar la cobertura al ámbito de datos o informaciones o Asecretos@ públicos y aumentar la dosimetría punitiva, relegando a la calidad de contravención contra la intimidad los aspectos netamente privados de la persona o la familia. Esta política criminológica del Estado, cuando menos, vulnera derechos fundamentales como el de igualdad (art.13), el debido proceso (art.29) y el de favorabilidad (art. 29 *in fine*), pues *A también es cierto que el principio de favorabilidad está esencialmente concebido para resolver conflictos entre leyes que coexisten de manera simultánea en el tiempo@* [64]. Uno de los fines esenciales del Estado, es la eficacia de los derechos, deberes y principios consagrados en la Constitución (art.2) y siempre prevalecerá los derechos inalienables de la persona (art.5) [65].

5. EL DELITO DE LOS DATOS PERSONALES REGISTRADOS EN FORMA AUTOMATIZADA CONTRA LA INTIMIDAD EN EL CODIGO PENAL ESPAÑOL DE 1995.

5.1. Estructura General del delito.

5.1.1. Notas preliminares básicas.

En este apartado no pretendemos diseccionar finamente los pormenores de los delitos

---

(63) Véase, aparte 4.2.4, punto 1.1. Delitos de los datos o informaciones automatizadas.
(64) Vid. C. Const., Sent. T-430, Jul. 1/90. M.P. Eduardo Cifuentes .
(65) Vid. C. Const., Sent. T-490, Ago.13/92. M.P. Eduardo Cifuentes.

contra *la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio*, previsto en el Título X, arts. 197 a 201, del Código Penal Español de 1995, sino sólo aquéllos delitos denominados contra *los datos personales registrados en forma automatizada (informática y/o telemáticamente) contra la intimidad*, que aúnestando subsumidos en el título mencionado, constituyen una vertiente plenamente identificable dentro del contexto, entre otras razones, por las siguientes:

a) Porque como lo ha determinado el Tribunal Constitucional Español, al analizar la influencia actual de la informática con relación al derecho a la intimidad prevista en el art. 18.4 CE, concluyó que se ha

> *incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama *la informática+* [66].

b) El bien jurídico objeto de tutela estatal en el título X del Código Penal Español de 1995, es sin lugar a dudas la *Intimidad*, como derecho fundamental, autónomo y limitado de la persona, o como genuinamente se concibió en el ensayo de Warren y Brandeis: un derecho a la A*inviolabilidad de la persona@*, que incorpora; por un lado, las facultades de no hacer, de abstención o de exclusión (en términos de Cooley, *Right to be let alone)* de cualquier atentado contra de A *la dignidad y la convivencia de un individuo en la sociedad o en sus relaciones sociales y familiares @* [67]; y de otro, el derecho precisado años más tarde por *Westin* y consistente en el derecho al control a la información referente a uno mismo (*A Right to control*

---

(66) Cfr. Sentencia de Julio 20 de 1993, Tribunal Constitucional Español. M.P.: García Mon., Fundamento Jurídico (FJ 6). AA.VV. *Colección de discos de Aranzadi*. Ed. Aranzadi, Pamplona (Esp.), 1997. Planteamientos que aceptamos con la excepción de considerar a la Alibertad informática@ como derecho nuevo, por los argumentos vertidos en la Parte II de esta investigación.

(67) WARREN, Samuel y BRANDEIS, Louis. ***El Derecho a la intimidad***. Edición a cargo de Benigno Pendás y Pilar Baselga. Ed. Civitas, S.A. Madrid, 1995. AThe Right to Privacy@, 1890. Veáse,Parte I.de este trabajo, en el que comentamos el Ensayo y extractamos las facultades negativas (derecho a no ser molestado) y positivas (derecho a control de la propia información) que más tarde los doctrinantes italianos (v.gr. Frosini y Losano) y españoles (Pérez Luño y Truyol y Serra), llamaran sobre todo, a las segundas, *libertad informática*. Los planteamientos de Frosini, en Vid. FROSINI, V. ***Informática y derecho.*** Ed. Temis, Bogotá, 1988, pág. 64.

information about oneselft). Este última faceta de la intimidad se potenciaría con el advenimiento de las nuevas tecnologías de la información y comunicación (TIC) y la informática , a partir de la segunda mitad del s. xx., como hemos anotado en esta investigación; y sobre todo cuando la *información* potencia su esencia conceptual de ser todo aquello que *nos pro-porciona conocimiento* [69] y por ende, protegible y/o vulnerable.

c) Recientes decisiones del Tribunal Constitucional Español (SSTC 254/1993 , Mayo 9 de 1994, Enero 13 de 1998 y Marzo 16 de 1998), enfatizan que Ael art. 18.4 de la CE incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona: derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos@. Así como que la *libertad informática* A*es un derecho a controlar el uso de los mismos datos insertos en un programa informático* (*habeas data*)@ .

.

d) Porque los denominados delitos de los datos de carácter personal contra la intimidad son conductas típicas surgidas como producto indefectible y concomitantemente con las nuevas tecnologías de la información y la comunicación (TIC), en las modernas *sociedades de la información* [70], y en los que los sujetos emplean medios comisivos o de ejecución del *iter criminis* de naturaleza electromagnética o computacional y dispositivos o aparatos informáticos y/o telemáticos.

---

(69) *A*El concepto se refiere a los seres humanos, pero puede extenderse también a los ordenadores o, en general, a cualquier sistema con posibilidad de percibirla y en consecuencia variar su estado. El receptor de la información, con su capacidad de asimilación (bien sea incremento de conocimiento, o cambio de estado) es, pues, una parte esencial del concepto. Otra lo es el lenguaje que aporta la información, compuesto de elementos perceptibles a través de los sentidos (o sensores, en el caso de una máquina) del receptor. Y, naturalmente, si hay mensaje habrá también un emisor, a veces otra persona pero, en términos más generales, un sistema que, como el receptor, es dinámico.@ Cfr. FERNANDEZ BEOBIDE, César. *Las nuevas tecnologías y las creaciones intelectuales. Aspectos positivos.* En: El Derecho a la propiedad intelectual y las nuevas tecnologías. Mincultura, Madrid, 1996, pág.51 y ss.

(70) ALa denominada *sociedad de la información* no es la fantasiosa idealización de un mundo futurista, sino una realidad de nuestros días, aunque todavía se encuentre en un estado embrionario comparado con lo que puede depararnos dentro de pocos años. Muchos de los elementos de esta sociedad de la información son suficientemente conocidos y prestan ya útiles servicios a la sociedad: el teléfono, las emisoras de radio y televisión inalámbricas y por cable, los satélites, las comunicaciones, las bibliotecas, las librerías, las bases de datos accesibles a distancia, y redes informáticas como Internet. Hasta el momento, en términos generales puede afirmarse que estos distintos elementos para vincular la información funcionan aisladamente, sin ningún tipo de interacción entre ellos@. Sin embargo, creemos que, hoy por hoy, existe tal interactividad gracias a la unión de las telecomunicaciones y la informática, con el descubrimiento de la *multimedia* que incorpora imágenes, sonidos y datos, digitalizados o no, con acceso lógico y/o físico a distancia (redes informáticas) o localmente (equipos computacionales personales, institucionales o empresariales). Vid. GOMEZ SEGADE, José. Respuestas de los sistemas de propiedad intelectual al reto tecnológico. El derecho europeo continental y el derecho anglosajón del Copyright. Mincultura, Madrid, 1996, pág. 131 y ss.

e) *Los términos iusinformáticos: datos de carácter personal*, fichero automatizado o bancos de datos, tratamiento de datos, responsable del fichero, *afectado* (por titular o interesado) y procedimiento de disociación se interpretan en el Código Penal Español, con base en la normativa extrapenal, básicamente en el Convenio del Consejo de Europa de 1981 y la Directiva del Parlamento Europeo y del Consejo de la Unión Europea de 24 de octubre de 1995, relativas 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 como no, en las definiciones que la LORTAD, trae en el artículo 31, pues se ha hecho una práctica inveterada que el legislador acuda a definiciones técnico-jurídicas, que aunque en no pocas veces producen colisiones o dificultades en su comprensibilidad diáfana al operador jurídico, resulta a la vista de la visión iusinformática de los derechos y libertades fundamentales --como hemos comentado en la Parte I y III-- el glosario mínimo necesario que aquél debe observar para la interiorización de la norma jurídica, la técnica TIC y la informática , y sobre todo para discernir el espíritu de la norma jurídica y aplicarla en cada caso *sub judice* en un momento histórico determinado.

Como analizamos en la Parte I, de este trabajo La Directiva 95/46/CE y la Directiva 97/66/CE, amplían el glosario de definiciones aplicables al procedimiento de ingreso, tratamiento, divulgación y teletransmisión y protección de datos de carácter personal, ya que el fenómeno TIC y la informática, día a día evoluciona y las ciencias jurídicas deben asimilar esa evolución reflejándola en los términos jurídico-técnicos: interesado, tratamiento (por almacenamiento, registro, transmisión, difusión, interconexión, bloqueo, supresión o destrucción, etc), fichero, responsable del tratamiento (más amplio que el del fichero), encargado del tratamiento, tercero, destinatario y consentimiento del interesado (como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan) [71]. Por tanto, el operador jurídico en las áreas del derecho civil, administrativo y penal deberá acudir a ellas cuando se trate de aplicar una interpretación mínima o gramatical para escrutar el espíritu de las normas jurídicas referentes a la visión iusinformática de los derechos.

f) En la visión iusinformática de los derechos se parte del concepto tradicional de

---

(71) La Directiva 95/46/CE, art. 2 . Cfr. AA.VV. ***Compedio de discos de CELEX, Bruselas*** (B), 1997.

documento impreso, escrito o *similares* para definir y precisar el concepto de docu*mento informático* contenidos en *soportes o aplicaciones informáticas y electrónicas (v.gr.ALos mensajes de correo electrónico@) o telemáticas* (no sin alguna resistencia teórica v.gr. El Internet y la problemática de los derechos fundamentales en el *ciberespacio:@Netlaw@*[71], Los documentos EDI: Electronic Data Interchange o IED: Intercambio electrónico de datos)[72], como objetos materiales sobre los que recae la actividad ilícita de *apoderamiento (por acceso), utilización, modificación* de datos reservados con carácter personal, o a los cuales se *accede* para *alterar o utilizarlos* en perjuicio del titular de los datos o de un tercero.

Tanto la jurisprudencia como la legislación han reconocido la existencia de los llamados documentos informáticos, electrónicos y telemáticos. En efecto, el Tribunal Supremo de España, Sala 20 en sus múltiples decisiones ha reconocido la existencia de los *documentos informáticos*, a partir del concepto de documento impreso, escrito, similar o tradicional (STSS 19/04/91. FJ.4. M.P. Soto Nieto; 14/11/93.FJ.3. M.P. Puerta Luis; y, 3/06/94. FJ.1. M.P.Martín Canivell; entre otras.), o bien aplicando el art. 26 del nuevo C.P.Esp de 1995 (STSS: 10/07/96. FJ.6.M.P: Soto Nieto; 121/1997, y 3/2/97.FJ.2, M.P:Joaquín Delgado García); pero al fin y al cabo, *documento informático* desde el punto de vista del hardware y software[73], como precisaremos al final de éste trabajo.

---

(71) Veáse, BARNES VASQUEZ, Javier. *La internet y el derecho. Una nota acerca de la libertad de expre sión e información en el espacio cibernético. En:* Cuaderno de Derecho Judicial. C.G.P.J., Ordenación de las telecomunicaciones No.VI, Madrid, 1997, Pág. 241 y ss.

(72) Veáse, la parte tercera de éste trabajo sobre el tema: Los datos informáticos, electrónicos y/o telemáticos. Los ficheros y/o bases de datos. Jurisprudencia sobre el documento informático. APodemos definir el IED como el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o administrativas. Un sistema de este tipo ha de cumplir tres requisitos básicos: a) el intercambio se ha de realizar por medios electrónicos, b) el formato tiene que estar normalizado, y c) la conexión ha de ser de ordenador a ordenador.@ Vid. DEL PESO NAVARRO, Emilio. *Resolución de conflictos en el intercambio electrónico de documentos. En:* Cuaderno de Derecho Judicial. C.G.P.J., Ambito jurídico de las tecnologías de la información.No.XI, Madrid, 1996, Pág.199 y ss.

(73) El Tribunal reiteradamente ha sostenido: AA) Que exista un documento, lo que equivale: a) Que se trate de un documento en sentido estricto, y ha de entenderse por tal el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un disquete, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como *cualquier cosa que sirve para ilustrar o comprobar algo+ (obsérvese que se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el operador del derecho tener en cuenta la evolución social), siempre que el llamado *documento+ tenga un soporte material, que es lo que sin duda exige la norma penal (por todas, TS SS 1114/1994 de 3 Jun., 1763/1994 de 11 Oct. y 711/1996 de 19 Oct.).@ STS Nov. 23 de 1996. M.P. Montero Fernández. FJ. 6.A. Cfr. AA.VV. Compendio discos Aranzadi. Ob. cit., Madrid, 1997.

Por su parte, la Ley 30 de 1992, Ley de Régimen jurídico de las administraciones públicas y del procedimiento administrativo común (LPRJPA, antes LPA), al regular las relaciones de los ciudadanos con la Administración General del Estado, destaca la incorporación de las nuevas tecnologías TIC en vida iuadministrativa y, particularmente denota, la A*validez y eficacia de documento original* A a los obtenidos con A*medios electrónicos, informáticos o telemáticos*@. Si bien la existencia de éstas modalidades de documento informático se hallan curiosamente desintonizadas con la LORTAD, a pesar creemos que en la realidad y práctica normativa deben no sólo sintonizarse sino de expedirse por el mismo año y fecha [74] y regular el fenómeno TIC en el derecho, interpretarse hermenéuticamente como norma extrapenal que ayuda a entender los términos técnicos que el C.P.Esp., emplea en el Título X, aparentemente divorciado de éstos.

g) Por referirse al descubrimiento y revelación de *secretos documentales informáticos,* sin consentimiento del titular, como una gama de las variopintas previstas en el tipo penal muy amplio que las protege: art. 197 del C.P.Esp. [75];

h) Por referirse al control auditivo o audiovisual clandestino de datos de carácter personal [76] a través de la interceptación con medios electromagnéticos que unen las telecomunicaciones y la informática (v.gr. TIC-Interactivo: Imagen, sonidos y datos: La multimedia); y,

i) En cuanto a los sujetos activo y pasivo; los verbos rectores (apropiar, usar, utilizar, interceptar, acceder, revelar, descubrir, divulgar); la base normativa penal y extrapenal (LORTAD, L.O 5/1992, de Oct. 29; Directiva 46/95/CE; Convenio Europeo de 1981); las modalidades de las conductas agravadas del tipo penal básico (v.gr. Si se realizan por personas responsables o encargados de ficheros, personas menores o incapaces, por cometerse en los *datos*

---

(74) GONZALEZ NAVARRO, Francisco y GONZALEZ PEREZ, Jesús. *Comentarios a la Ley de Régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.* Ed. Civitas, S.A., 1a, ed., Madrid. 1997, pág. 695.

(75) SERRANO GOMEZ, Alfonso. *Delitos contra la intimidad , el derecho a la propia imagen y la inviolabilidad de domicilio. En*: Derecho Penal - Parte Especial. Ed. Dykinson, Madrid, 2da. ed., 1997, pág.227.

(76) MORALES PRATS, F. *Delitos contra la intimidad*... Ob. ut supra cit., pág. 303 y ss.

sensibles [77], --por regla general, exentos de tratamiento automatizado, según las normas comunitarias--, o con fines lucrativos), y la penalidad, son similares a los aplicados para los delitos contra la intimidad y demás derechos de la persona humana, estipulados en el Título X, del C.P.Esp. Igualmente, y sobre éste último aspecto, particularmente en cuanto a la gravedad de las penas que se establecen para casi todos los supuestos pueden llevar en algún caso a violar el *principio de culpabilidad*, pues a la infracción cometida se le fija una pena desproporcionada [78], como puntualizaremos más adelante.

5.1.2. Tipos delictivos.

El delito de los datos o las informaciones de carácter personal que atenta la visión iusinformática del derecho fundamental a la intimidad de las personas en la estructura actual del Título X, Cap. I del C.P.Esp. de 1995, es un planteamiento doctrinal que pretende mostrar el cúmulo de figuras delictivas (previstas o no en la legislación penal [79]) saturadas o condicionadas por las nuevas tecnologías de la información y la comunicación (TIC) y los medios automatizados electromagnéticamente. Es decir, aquellos tipos delictivos denominados de *Descubrimiento y Revelación de Secretos*, a través de medios informáticos y/o telemáticos que *A el legislador regula... de una forma realmente complicada, con algún artículo interminable y de*

---

(77) La Directiva 95/46/CE, les concede una categoría especial de tratamiento, a los datos personales que Arevelen el 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@, prohibiéndolo por parte de los Estados (art.8.1), salvo que se de una cualquiera de las excepciones previstas en los numerales 2 a 7. v.gr. que haya consentimiento explícito del interesado; que sea necesario para salvaguardar el interés vital del interesado o de otra persona, etc. En todo caso, estas excepciones son taxativas o *numerus clausus.* Vid. Compendio CELEX. Ob. cit. Bruselas, 1997. En la Ley de Protección de la Intimidad del Canadá, AAct Privacy@ 1983, se incluyen los denominados Adatos sensibles@ dentro de un extenso listado en el art.3, en trece literales, como datos personales o informaciones de carácter personal v.gr. (a) la información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona. La naturaleza de sensibles o de limitada o prohibido descubrimiento, se determina por la condición de ser datos a los que les falta el consentimiento del titular, se hallan bajo el control del Estado y constituyen una causal de excepción (numerus clausus) según el art. 8.1 y 2. LPDPC**.** Cfr.Caso: Mackenzie v. Canada (Ministerio de Salud Nacional y Bienestar Social). (1994), 88 F.T.R. 52; 59 C.P.R. (3d) 63 (Corte Federal, Primera Instancia). AA. VV. *Base de Datos de la Univ. de Montreal. Biblioteca Virtual de Derecho Público. (C).* Vía Internet en Inglés, Montreal (Canadá), 1998.

(78) Penas. SERRANO GOMEZ, A. Ob. cit. pág. 226.

(79) a) La creación ilegal de ficheros automatizados de datos sensibles y no solamente la penalización de los que revelen estos datos (art.197.5.); b) La obtención por medios fraudulentos, desleales o ilícitos o sin menoscabar el consentimiento de la persona afectada, de este tipo de datos (sensibles) para incluirlos en ficheros automatizados. Vid. BAON RAMIREZ, Rogelio. ***Visión general de la informática en el nuevo Código Penal.*** En: Cuadernos de Derecho Judicial. C.S.P.J., Ambito de las tecnologías de la información. No. XI, Madrid, 1996, pág. 95:

difícil concreción, lo que lleva a la inseguridad jurídica@ [80]. Súmese a ello, que en el art. 197.1 del C.P.de Esp., contiene objetos materiales del hecho punible, como los llamados A*mensajes de correo electrónico@,* que técnica, jurídica, sistemática e iusinformáticamente mejor ubicados quedarían en el numeral 2 del art. 197. Igualmente el art. 197.2 id., contiene acciones punitivas sinónimas al tipificar doblemente la *Autilización de datos@,* tanto en el apartado primero como en el segundo. Estos y otros aspectos que son aparentemente son fruto del A*desconcierto y la precipitación (lo que) han presidido la creación de este precepto@* [81], tal como precisaremos y ampliaremos

Pese a ello, y a la vista de la actual redacción que el C.P.Esp., se erigen los Delitos de ADescubrimiento y Revelación de Secretos@ contra la intimidad y el derecho a la propia imagen (Tit. X). Las tipos delictivos básicos de los delitos que llamamos de los datos o informaciones de carácter personal contra la intimidad, previa la transcripción de la norma penal vigente, son:

> **Art. 197-1**. *El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*.

a) Delito de Acceso a los documentos informáticos (Amensajes de correo electrónico@) en soportes electrónicos, previsto en el art. 197.1, *ab initio* del C.P.Esp.más adelante.

b) Delito de interceptación de documentos informáticos en soportes electrónicos o telemáticos, previsto en el art. 197.1, *in fine* del C.P.Esp.

> **Art. 197-2.** *Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*

---

(80) Cfr. SERRANO GOMEZ, A., Ob. ut supra cit. pág.226

(81) MORALES PRATS, Fermín. ***La protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995.*** En: Revista C.G.P.J. Delitos contra la libertad y la seguridad, Madrid, 1996, pág.173 y ss.

c) Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar registrados en documentos informáticos, electrónicos o telemáticos, previstos en el art. 197.2 Id.

Los tipos delictivos agravados, son:

> **Art.197- 3.** *Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

a) Por la difusión, revelación o cesión a terceros de datos informáticos y/o telemáticos (art. 197.3. *ab initio*).

> **Art.197-4.** *Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.*

b) Son dos tipos agravados fundidos en un inciso, con diferente pena: El primero, por la condición calificada del sujeto activo del delito al actuar como encargado o responsable del fichero o banco de datos informatizados o telemáticos (art. 197. 4. *ab initio*). El segundo, por la conducta subsiguiente realizada por el sujeto activo, es decir, por la difusión, cesión o revelación de los datos (art.197.4 *in fine).*En este última caso la pena es super agravada.

> **Art. 197-5.** *Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.*

c) Son dos tipos agravados fundidos en un mismo inciso, con igual pena aumentada, por la afectación y calidad de los datos y la *capitis diminutio* de la víctima: El primero, por la afectación a los datos de carácter personal, considerados A*sensibles*@ o constitutivos del *Anúcleo duro*@ de la intimidad (art. 197.5, *ab initio* del C.P.Esp). El segundo, es por la condición cualificada de la víctima del delito (ser menor o incapaz), según el art. 197.5, *in fine* del C.P.Esp.

Art. 197-6. *Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 a 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.*

d) Nuevamente son dos tipos agravados en un mismo inciso, con diferente pena impuesta, pero en la parte *in fine* se establece un tipo agravado potenciado de ultraprotección, se entiende, a los datos sensibles y no a la condición de *capitis diminutio* de la víctima. El primero, será por la realización con fines lucrativos de los tipos básicos a), b), c) y/o los tipos agravados previstos en el literal a), b), c) --art. 197.6 *ab initio*--. El segundo, se entiende un tipo ultragravado --si nos permiten el término--, si se realiza además del fin lucrativo sobre los datos sensibles, es decir, contra la ideología, religión, creencias, salud, origen racial o vida sexual (art. 197.6. *in fine).*

> **Art. 198.** *La autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualesquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.*

e) Por la condición calificada del sujeto activo, al actuar como autoridad o funcionario público, en circunstancias especiales y prevaliéndose de su cargo y con imposición de penas principales (prisión) y accesorias (inhabilitación absoluta del cargo) --art. 198 C.P.Esp.--

Como tipo atenuado del tipo agravado previsto en el art. 197.3. C.P.Esp.

> ***Art. 197. 3. Parte In fine****. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que con conocimiento de su origen ilícito y sin haber tomado parte de su descubrimiento, realizare la conducta descrita en el párrafo anterior.*

f) Es el tipo atenuado por la difusión, revelación o cesión a terceros de datos informáticos y/o telemáticos, que requiere para su configuración, lo siguiente: a) Conocimiento del origen ilícito de los datos, b) No tomar parte en el descubrimiento o revelación de los mismos, c) Realizar las conductas previstas en la parte *ab initio* del art. 197.3, es decir, la difusión, revelación o cesión a terceros de los datos (Art. 197.3. *ab initio*) y d) La pena impuesta es menor que la impuesta al tipo agravado del art. 197.3 *ab initio,* pues se disminuye de dos a cinco, a uno a tres años de prisión.

5.2. Delito de acceso, utilización y alteración de datos o informaciones de carácter personal o familiar registrados en documentos informáticos o de interceptación de documentos electrónicos o telemáticos.

Este delito se encuentra previsto en el art. 197.2 del C.P. Esp., y tipifica conductas tendientes a descubrir los secretos o vulnerar la intimidad del titular de los datos o de un tercero, por quien, sin estar autorizado, accede (o A*apodere*@, según la redacción gramatical, pero impropia a la utilizada por la LORTAD [8 2]), utilice, modifique o altere datos o informaciones de carácter personal o familiar que se hallen registrados en ficheros o bancos de datos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

En la redacción actual del art. 197.1, *ab initio* C.P.Esp., se tipifica el delito de A*apoderamiento de papeles, cartas, mensaje de correo electrónico o cualesquiera otros documentos o efectos personales@.* Sin embargo, los mensajes de correo electrónico, como se ha sostenido en la parte tercera de éste trabajo, son una modalidad de documentos informáticos, y más concretamente electrónicos o telemáticos. En tal virtud, desde el punto de vista técnico, jurídico e iusinformático, dichos documentos muestran ajenidad sistemática al incluirlos en la parte inicial del art. 197.1, cuando mejor ubicados quedarían en el numeral 2 del art. 197, dentro del género de documentos informáticos y/o telemáticos que el legislador del 1995, bien acoge sin entrar a enlistar o enumerarlos taxativamente o con el sistema *numerus clausus,* como muestra palmaria de que el fenómeno tecnológico de la información y la comunicación (TIC), en esta sociedad informatizada está en constante crecimiento y evolución que no permite cláusulas y términos cerrados para describirlos fidedignamente.

Sin embargo, se diría que el término *o cualesquiera otros documentos*, previsto en el art.197.1., incluiría a los todos los documentos (escritos o por sistemas tradicionales de impresión, como los informáticos y/o telemáticos) y que de nada valdría eliminar el término *mensajes de correo electrónico (E-mail)*, del numeral primero, pues seguirían estando incluidos por el

---

(82) Siendo la LORTAD (LO. 5/1992), el Convenio Europeo de 1981 y la Directiva 95/46/CE, además de ser normas de protección extrapenal de la intimidad son normas de interpretación de la terminología utilizada por el C.P.Esp., en lo referido al Tit. X, debemos en consecuencia atender sus conceptos y estructura normativa y sistemática para entender mejor el fenómeno TIC y su incidencia en los Delitos contra la intimidad. Por ello, se ha sostenido con razón que A...la acción de apoderamiento de datos (expresión impropia la vista de los conceptos informáticos que emplea la LORTAD) tiene como traducción técnica más ajustada la acción igualdad de penas pero con diferente tratamiento jurídico penal a un misma conducta y verbo Autilizar@ datos. Cfr. MORALES PRATS, F. Ob.ut supra cit., pág.173.de acceso a los mismos, que es la tipificada en el inciso segundo@ parte in fine, con

término genérico de Adocumentos@, lo cual no es correcto, ya que los *documentos informáticos y/o telemáticos,* si tienen expresa referencia en el art.197.2 C.P.Esp., lo cual los descarta de la previsión general del numeral 11. Por lo más, el término empleado en el numeral 11, se refiere a todos aquellas formas de documentos escritos o impresos, conocidos o conocibles en el futuro; por lo menos, a los diferentes de papeles o cartas.

Este es otro argumento interpretativo gramatical de la ajenidad de los men- sajes de correo electrónico en el numeral 1 del art.197 C.P.Esp., pues de lo contrario se daría la paradoja jurídica de estar ubicado doblemente un mismo objeto material del delito [83] (Amensajes de *correo electrónico*@ en el numeral 1 y 2), con diferente tratamiento jurídico aunque con igual sanción punitiva.

En efecto, sin desconocer la autonomía de tipificación ni la redacción gramatical empleada por el actual C.P.Esp., tanto para el delito de apoderamiento de papeles, cartas, mensajes de correo electrónico o documentos y que la doctrina califica de *delitos sobre secretos documentales* [84], para diferenciarlo del delito de *apoderamiento (por acceso), utilización y alteración de datos registrados en documentos informáticos y/o telemáticos,* que la doctrina iuspenalista llama de *AAbusos informáticos@*[85], creemos a la vista de las razones antes dadas, que para tratar el fenómeno TIC y los delitos contra la intimidad, podemos plantear el *Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar registrados en documentos informáticos (art.197.2),* en una primera parte y el *de interceptación de documentos electrónicos o telemáticos (art.197.1 in fine),* en una segunda parte, en atención a una mejor sistematización

---

(83) Sin embargo, recurriendo a la una aclaración interpretativa, se ha sostenido que el Aprimer pasaje del art. 197.1 C.P., debe limitarse a las conductas de apoderamiento por medio de conexión del ordenador a la red telefónica (correspondencia informática) ya impresos fuera del sistema. Asimismo el tipo puede ser proyectado a la conducta de captación intelectual, sin desplazamiento ilícito, de los referidos mensajes (por ejemplo, cuando se hallan en pantalla de ordenador)@. A pesar de ello, la excepción no justifica la separación de la interpretación del objeto material del delito por estar dentro o fuera de un sistema tecnológico. Cfr. MORALES PRATS, F. Ob. ut supra cit., pág. 300.

(84) Vid. MUÑOZ CONDE, Francisco. ***Derecho Penal. Parte Especial.*** Undécima ed., Ed. Tirant lo blanch, Valencia, 1996, pág.218. SERRANO GOMEZ, A. Ob. cit., pág. 227.

(85) Cfr. MORALES PRATS, F. *Comentarios a la parte Especial del Derecho Penal* ... Ob. cit.pág. 229. Igual En: ***La protección penal de la intimidad...,*** ALa protección penal de la Aprivavy@ informática: Ahabeas Data@ y represión penal de los abusos informáticos. El CP de 1995 en el art. 197.2. contempla la tutela penal de la Aprivacy@ informática por primera vez en nuestro país...@ Ob. cit., pág. 165.

de los documentos informáticos y/o telemáticos, con la aclaración de que una y otra figuras punitivas, están referidas a la visión iusinformática del derecho a la intimidad personal y familiar, pues de lo contrario, nos estaríamos refiriendo: o, a los delitos *contra los datos informáticos* previstos en el C.P.Esp., para otros bienes jurídicos como el Patrimonio y el orden socioeconómico (Tit.XIII), v.gr. delitos de destrucción, alteración, inutilización de datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos (ADelito de Daños@, art. 264.2), o a cualquier otro tipo o bien jurídico penalmente tutelado.

Ahora bien, por regla general, la teletransmisión de datos o informaciones se realiza entre máquinas automatizadas a través de medios o equipos electromagnéticos o computacionales con el auxilio de soportes (hardware y/o software) informáticos y/o telemáticos y su producto en consecuencia es de idéntica naturaleza tecnológica (El documento telemático), y por tanto, la transmisión, emisión y la recepción de los datos o informaciones, se presenta en la memoria de los discos electromagnéticos conocidos (fijos o removibles de diferente formato: *disquettes,* CD´s, CD-ROM, CD-RAM, CD-I, DVD) o conocibles en el futuro (p.e. evolución del DVD); en las unidades periféricas computacionales (como impresoras, grabadoras de sonido o audio-visuales, altoparlantes y aparatos audio-visuales, etc) o asimilables. La multimedia (que une telecomunicaciones e informática: datos, imagen y sonido), hace acopio de estas técnicas TIC en la actualidad y una de las formas de transmitir y recepcionar datos, imagen y sonido es a través del llamado documento electrónico de intercambio de datos A*EDI*@[86].

Ahora bien, la interceptación de las telecomunicaciones [87] utilizando A*artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o cualquier otra señal de comunicación*@, se ha tipificado en la parte *in fine* del art. 197.1 del C.P.Esp., como un

---

(86) Véase, apartado 5.5.1., d), sobre el EDI o IDE . Además: AA.VV. *El EDI (Electronic Data Interchange).* En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.pág.1

(87) El art 2.2 de la Ley 31 de 1987, estipula que Alos servicios de telecomunicación se organizarán de manera que pueda garantizarse eficazmente el secreto de las telecomunicaciones de conformidad con lo dispuesto en el art. 18.3 de la Constitución@. El art 3, de la ley sostiene que se entiende Apor telecomunicaciones: Toda transmisión, emisión, o recepción de signos, señales, escritos imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos@. Citado por SERRANO GOMEZ, A. Ob. cit. pág.226

delito mutilado o imperfecto de actos, que no requiere para la consumación el efectivo descubrimiento de la intimidad; basta así para colmar la perfección típica con la interceptación de telecomunicaciones o con la utilización de aparatos de escucha, grabación o reproducción del sonido o de la imagen o cualquier otra señal de comunicación, siempre que alguno de estos sea llevado a cabo con la finalidad de descubrir la intimidad de otro (elemento subjetivo del injusto)... [88]

En nuestro caso y sin desconocer la amplitud del tipo penal, nos remitimos sólo a la interceptación de los datos o informaciones de carácter personal contenidas en un soporte o documento telemático y con la finalidad de descubrir la intimidad de una persona, tras la denominación de *delito de interceptación de los datos o informaciones de carácter personal o familiar contenidos en documentos electrónicos o telemáticos (art. 197.1 in fine C.P.Esp.),* es decir, a aquellos documentos de intercambio de información o (EDI) o Aactos satélites@ en los cuales A*no se produce papel sino en registros informáticos de los mensajes que se emiten o recepcionan*@ [89].

5.2.1. Bien Jurídico Constitucional Protegido: La intimidad.

El derecho fundamental a la intimidad personal y familiar es el bien jurídico tutelado en el Título X del C.P.Esp., a partir de 1995. Esta prerrogativa, *sine qua nom* del bien jurídico y la condición de protección sólo de la persona humana, como sujeto físico (personal o grupo familiar, no extensible a otros grupos o entes sin personalidad v.gr. una comunidad de bienes) abre la puerta a la discusión hermenéutica de sí aquí también se incluye la intimidad de las personas jurídicas o morales, para las cuales la ley finge tienen similares atribuciones que la persona física, cuando en el art. 200 del C.P.Esp., extiende la tutela de la intimidad a las personas jurídicas. Algunos estiman que la nueva protección que brinda el CP a la intimidad, se extiende a las personas jurídicas A*al socaire, que no mandato del TC*...(por lo cual) *merece aplauso* [90]; otros, entendemos que la extensión a la protección penal de la intimidad de las personas jurídicas, al

---

(88) Cfr. MORALES PRATS, F. *Comentarios a la parte Especial del Derecho Penal* ... Ob. cit.pág. 305.
(89) Vid. AA.VV. *El EDI*... Ob. cit., pág 1 y ss.
(90) Cfr. QUERALT JIMENEZ, J.J. ***Derecho Penal Español.*** Parte Especial. 3 ed., Ed. J.M. Bosch, Barcelona, 1996, págs. 183 y 184.

menos en el Tít. X., quebranta la estructura sistémica del C.P., y desconoce la legislación comparada sobre el tema (EE.UU., Alemania, Francia), el concepto genuino de la intimidad como derecho derivado exclusivamente de la persona humana y prevista en el art. 18 C.E. y reglamentado en la LORTAD, especialmente en el art.3,a) LORTAD, como un derecho de la personalidad exclusivo de los seres humanos y no atribuible a las personas morales o jurídicas, aunque no se desconoce que éstas tengan otros derechos de naturaleza no fundamental o de la personalidad, fundados en la dignidad, prestigio o autoridad moral, según el Tribunal Constitucional (STCS, 06/8/1988, 11/11/91) y otros mecanismos de protección civil (art.1002 C.c.), según el Tribunal Supremo [91], o derechos que por ficción legal se han atribuido a las personas jurídicas, como si fueran físicas de los cuales en todo caso, se excluyen los de potestad y carácter de personalísimos, como la intimidad. El Convenio de Europa de 1981 y la Directiva 95/46/CE, sobre el tema es concordante al deferir éste derecho a la intimidad como un derecho exclusivo de las personas físicas.

A pesar de todo, con la protección a la intimidad de las personas jurídicas --se dice--, se brinda una interpretación delimitada para éstas, pero también discutible: primero, porque se hace acopio de una Acláusula de extensión de la tutela penal@, al aclarar que si bien las personas jurídicas no tienen intimidad, sí la poseen las personas físicas que la representan, pero siendo así, el régimen jurídico no es el de las personas jurídicas sino el de las personas físicas, ubicado en diferente parte y bajo diversos bienes jurídicos tutelados por el C.P. Y, segundo, porque la interpretación. del art. 200 del C.P.Esp. con relación al art. 278, basado en la frase *in fine* que aquel contiene: A*salvo lo dispuesto en otros preceptos*@, debe llevarnos a reconocer que el legislador ha generado A*una grave laguna*@, al no preveer A*atentados a la información empresarial reservada mediante abusos informáticos, puesto que no alude a medios comisivos del art. 197.2 C.P.@, y* por tanto , el art. 200 A*no cumple una función subsidiaria, de recogida de conducta no abarcadas en el art. 278 CP. Así, el art. 200 CP, acogería conductas ilícitas de descubrimiento y*

---

(91) Citando a PEREZ CANOVAS, apoya la posición de que Alas personas jurídicas y el derecho al honor (o prestigio como lo denomina el Tribunal Constitucional): Comentario a la S.T.S. de 5 de octubre de 1989". ORTI VALLEJO, Antonio. *Derecho a la intimidad e informática*. Ed. Comares, Granada (Esp.), 1994. págs.74 y ss.

de revelación o cesión de datos automatizados de personas jurídicas (en relación a los núms. 2 y 3 del art. 197 CP) *pero al precio de desconocer su ubicación sistemática entre los delitos contra la intimidad de las personas*@ [92].

En consecuencia, al estimar que el bien jurídico protegido en el Tít. X, es la intimidad de las personas, se pone fin a las interpretaciones doctrinales derivadas de los delitos contra la libertad de las personas (*Delitos contra la libertad y seguridad*), a las que se recurría en el anterior código penal para conceptualizar la intimidad como bien jurídico tutelable (art. 497ss) y en las que, por un lado, se hacía énfasis sobre la concreción necesaria que debía dársele a dicho bien jurídico en su funcionalidad y para evitar que todo delito se convierta en un hecho contra la intimidad [93]; y por otro, se posibilitaba la protección penal *inespecífica* de la intimidad, en forma limitada, fragmentaria [94] y no plena [95] y que quedáse

> anacrónico la protección a la intimidad frente al salto cualitativo de la tecnología, tanto en relación a los nuevos *procedimientos técnicos generales* para entrar en el ámbito físico y espiritual personal de otro, como los *procesos de informatización*, que permiten establecer una red que absorbe toda la experiencia personal del sujeto y la ajeniza [96].

Hoy por hoy, el derecho a la intimidad como reiteradamente lo ha sostenido el Tribunal Constitucional Español, no es un derecho absoluto, como no lo es ninguno de los derechos fundamentales, es un derecho limitado por la Constitución, la leyes y los demás derechos y valores constitucionales (art. 10.1-2 y 55.1CE) y como derivación de la dignidad de la persona, implica *la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana+ (STC 209/1988, FJ 3, STC, y Mayo 9 de 1994, FJ.6), pero además es un derecho en latente amenaza por lasnuevas tecnologías de la información y la comunicación (TIC), lo cual lo

---

(92). Cfr. MORALES PRATS, F. Ob. ut supra cit. pág. 338 y ss.
(93) Vid. BUSTOS RAMIREZ, Juan. *Manual de Derecho Penal. Parte Especial. 2da, ed.* Ed. Ariel S.A., Barcelona, 1991, pág.87.
(94) QUERALT JIMENEZ, J.J. ***Derecho Penal Español... Ob. cit., pág. 183.***
(95) Vid. GIL HERNANDEZ, Angel. *Protección de la intimidad corporal: Aspectos penales y procesales.* En: Revista General del Derecho. Año, LII Núm. 622-623, Jul-Ago., Valencia, 1996, pág. 7950 y ss.
(96) Véase, BUSTOS RAMIREZ, J. *Manual de Derecho Penal... Ob. cit., pág. 88.*

ha hecho un derecho altamente vulnerable a la par que potencialmente protegible por las normas civiles, administrativas y penales.

Por ello, y con mucha mayor razón, la famosa Sentencia de Julio 20 de 1993 y más recientemente la Sentencia de Mayo 9 de 1994 del TC., al desestimar un recurso de amparo sobre el régimen de obligatoriedad del NIF (Número de Identificación Fiscal Español) y de obtención de información con base en el mismo, contenido en el Real Decreto 338/1990, el cual, se decía, atentaba contra el derecho a la intimidad previsto en el art.18 CE (y en relación directa con el art. 18.4 id), reconoce el Tribunal Constitucional, la vulnerabilidad de derechos subjetivos e intereses legítimos como el grado de protección que debe garantizar el Estado en base a la Constitución, el Ordenamiento Jurídico interno y la interpretación hermenéutica de las normas, principios y tratados ratificados por España (art.10.2 CE), en cuanto se refieran al tratamiento automatizado de datos de carácter particular y los derechos fundamentales, y en especial, al derecho de la intimidad (Convenio Europeo de Dic. 27 de 1981. Hoy también, la Directiva 95/46/CE, del Parlamento y Consejo de Europa, que amplia y precisa aspectos del tratamiento de datos del Convenio y los demás instrumentos normativos comunitarios de desarrollo sobre el tema [97]) .

En el FJ.7, la STC 05/09/94, sostuvo al respecto:

Como ya se ha anticipado, cuestiona la demanda la legitimidad constitucional de una norma que, a través de un instrumento de recopilación de información, puede propiciar un uso desviado de ésta y, en consecuencia, la efectiva invasión de la esfera privada de los ciudadanos afectados. Desde luego, es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las

(97) Veáse, parte primera y tercera de éste trabajo. Además se debe destacar como lo sostiene el considerando 7 y 10, a saber: A7) las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;@ y A10. que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales@

*facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho (STC 254/1993). En este sentido se ha afirmado que, ya que *los datos personales que almacena la Administración son utilizados por sus autoridades y servicios+, no es posible *aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión+ (STC 254/1993, FJ7). En consecuencia con ello, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.*

5.2.2. Acceso, utilización. alteración e interceptación de datos contenidos en documentos informáticos.

5.2.2.1. Parte A*b initio* del tipo.

Para el *Delito de acceso, utilización y alteración de datos o informaciones de carácter particular o familiar* [98] *registrados en documentos informáticos* (art.197.2). La acción consiste en el acceso, la utilización y alteración de documentos informáticos, electrónicos o telemáticos, siempre que se hagan con la finalidad de descubrir secretos, sin posterior divulgación, que atenta contra la intimidad del titular de los datos de carácter personal o familiar o de un tercero y se hallen registrados.

En el titulo VI del Código Penal Canadiense destinado a los Delitos contra la Intimidad (A*Invasion Privacy*@), en los arts. 183 a 196, se estructura la figura penal básica de la interceptación (que subsume el acceso, utilización y alteración) de datos o informaciones (A*Interception of communications*@) de carácter particular, sin consentimiento del titular, o sin consentimiento de una de las partes cuando existe una comunicación hablada o escrito y por cualquier medio mecánico o eletromagnético. Así mismo se establece las excepciones a encasillarse en el tipo penal básico, por disposición legal o judicial, la interceptación de secretos o informaciones confidenciales y la interceptación de las telecomunicaciones por medios subrepticios

(98) MORALES PRATS, F., *Protección a la* ... Ob. cit., pág. 174 Critica el término ***familiar,*** porque considera una Amuletilla@ que trae el art.18 CE y que no ha podido desprenderse el legislador penal de 1995, a pesar de que la LORTAD, no menciona a los Adatos familiares@ sino únicamente los personales en las cuales obviamente están aquellos (art.3, a)). Sin embargo, esto no suma ni resta a la recta interpretación del derecho fundamental de la intimidad que abarca A aquella parcela de la personalidad que su titular puede mantener legítimamente al margen del conocimiento público, el denominado *ius solitudinis@, pues la intimidad es un bastión que se erige contra las intromisiones de los demás en la esfera privada de un sujeto, intromisión que puede sobrevenir tanto de los particulares como de los poderes públicos@. Cfr.* QUERALT JIMENEZ, J.J. Ob. cit., pág. 183.

mecánicos, acústicos o electromagnéticos, tal como vimos en el apartado 2.2. de éste trabajo. Sin embargo, la figura que más se aproxima a los tipo penal aquí analizado es la prevista en el art. 193.1, sobre el delito de A*Disclosure of information*@, que tipifica el delito de descubrimiento, revelación y utilización de datos o informaciones de carácter personal, sin el consentimiento expreso o tácito del titular, contra la intimidad y sea cual fuere el soporte en el que se hallen (documentos impresos, escritos o informáticos y/o telemáticos, al decir: A...*by means of an electro-magnetic, acustic, mechanical or other device*...@). En el mismo artículo expone las causales de excepción a los que no se aplica la norma, tales como, por ejemplo, cuando media un procedimiento civil, penal o de cualquier otra índole en los que se requiera alguna prueba contra la persona concernida con los datos (Subdivisión 2).

5.2.2.1.1. Acceso.

El tradicional *delito de apoderamiento* de papeles, cartas o *documentos en general* que contienen secretos y son objeto de descubrimiento, existe una clara, matizada y evolucionada jurisprudencia y doctrina, antes y después del C .P. de 1995[99]. Sin embargo, desde antes de la existencia del art. 197 del actual Código Penal, se planteaba la excepcionalidad referente al significado y significante del término *apoderamiento* aplicado a los documentos elaborados a través de Amedios tecnológicos modernos@ o informáticos y/o telemáticos que contenían secretos, pues se discutía si éstos eran o no objeto de aprehensibilidad material con igual criterio al aplicado al documento escrito, impreso o similares (v.gr. una fotografía, un plano, etc), o al menos se planteaba el anacronismo y la dificultad de aplicar el concepto de apoderamiento documental previsto en el ordenamiento jurídico a los documentos informáticos[100].

Hoy, la doctrina y jurisprudencia españolas, teniendo en cuenta que los documentos

---

(99) Es tal la evolución de la jurisprudencia que se extiende el apoderamiento a la Areceptación@, por error de correos, de cartas destinadas a otras personas y que luego son abiertas (STS 6/10/67, 25/11/69). AEl apoderamiento es tan fundamental, que si se pueden conocer los secretos documentales de otro sin apoderarse de sus papeles no existe este delito o, por lo menos, este tipo delictivo en concreto@. Cfr. MUÑOZ CONDE, Francisco. Ob. cit., pág. 218-219.

(100) Así se planteaba desde 1983, por MORALES PRATS, F. *La tutela penal de la intimidad: privacy e informática.* Barcelona, 1983, pág. 191-192. En igual sentido: BUSTOS R., Juan. *Manual*... Ob. cit., pág 88.

informáticos son una modalidad de documento, según las previsiones del art. 26 del Código Penal (STSS, Sala Penal: 9/05/94, 3/2/97), interpretan el concepto de apoderamiento utilizado en el art. 197, en un sentido amplio, que no solamente incluye al referente físico, sino al sentido lógico de conocimiento, es decir, que se puede aprehender no sólo lo material (aprehensión física u objetiva) sino lo que puede ser captado por el sistema sensorial humano, tal como las imágenes, datos y sonidos (aprehensión sensorial).

Si bien esto es cierto, no podemos desconocer que la conducta comportamental exigida por el art. 197.1 y 2., sobre el apoderamiento no sólo se aplica a los documentos escritos, sino a los no escritos e informáticos y por éstos últimos se impone que el término apoderamiento se ajuste a las nuevas tecnologías TIC que destaca la informática jurídica, el ciclo o fases de tratamiento automatizado de la información y la normas jurídicas penales y extrapenales (LORTAD, Directiva 95/46/CE, Convenio de 1981) sobre el tema. En efecto, A*la acción de apoderamiento de datos... tiene como traducción técnica más ajustada la acción de acceso a los mismos, que es la tipificada en el inciso segundo*@ **[101]** parte *in fine* del art. 197.

Ahora bien, para entender la punibilidad del acceso a los datos contenidos en documentos informáticos, veamos cuál es el ámbito normativo legal del derecho de acceso. Para ello recurrimos a las normas extrapenales (LORTAD, D.R..1332/1994, Directiva 95/46/CE). En efecto, mediante el derecho de acceso, se garantiza que:

> *1. El afectado (por el titular del derecho o interesado, según la Directiva 95/46/CE) tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados (o bancos de datos).*
> *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.*
> *3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes (art. 14, LORTAD). -- paréntesis nuestros--*

Este derecho personalísimo de acceso a los datos o informaciones (legibles o inteligibles _____

(101) Cfr. MORALES PRATS. *Protección a la* ... Ob. cit., pág 173.

) automatizadas, que le conciernen al titular o interesado, es parte integrante del derecho de *habeas data* junto al de actualización, rectificación y cancelación de datos y desde el punto de vista formal se configura siempre que la solicitud o petición reúna los requisitos legales de forma y de fondo, se ejercite *in témpore* o se demuestre un interés legítimo (arts. 14 a 16, LORTAD). Este derecho ha sido objeto de puntuales reglamentaciones, sobre todo de *tipo procedimental*, tal como lo confirma la exposición de motivos del Real Decreto 20/6/94, Núm. 1332/94, a efectos de completar el ámbito, esencia y grado de protegibilidad del derecho, y por ende, para que el interesado solicite la consulta de los ficheros o bancos de datos, por medio de la visualización en pantalla, la comunicación escrita, impresa, copiada, telecopiada, certificada por correo, *o cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo* (art. 12 Id.).

El derecho de acceso a los datos de carácter particular registrados, bajo las anteriores condiciones y requisitos, sólo puede ser negado, cuando los ficheros siendo de titularidad pública se dé alguno de los siguientes supuestos: a) Por el factor temporal o de legitimidad previsto en el art.14.3, b) Por el factor de acentuada protección de los *ficheros de las fuerzas y cuerpos de seguridad* en la recogida y tratamiento automatizado y del que pudieren derivarse riesgos 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 realizado (art.20 y 21.1); c) Por el factor de protección de las funciones administrativas tributarias en los ficheros de la Hacienda pública (art. 21.2); y, d) Por el factor de ponderación de los intereses público o de terceros más dignos de protección, previstos en el art. 22.2 de la Ley Orgánica 5/1992; o, finalmente y siendo los ficheros de titularidad privada, cuando la solicitud sea formulada por persona distinta del *afectado* o interesado (art. 14 D.R.1332/1994).

En la ley 30/1992, *Ley de Régimen jurídico de las administraciones públicas y el procedimiento administrativo común* (LRJPA), hermana pero desconectada en la esencia y objeto material de regulación con la LORTAD, como antes indicábamos al tratar los documentos informáticos, regula el derecho de acceso de los ciudadanos ante las administraciones generales del Estado (art.105 b), CE) y por tanto, debe servir de norma extrapenal, para entender la licitud e ilicitud del mentado derecho, y en particular cuando se acceda a documentos informáticos o telemáticos que se encuentren en *archivos o registros públicos* (art.197.2 *ab initio* C.P.Esp).

En efecto, el art. 37 y 45 de la LRJPA, se regula expresamente el derecho de *habeas data* que incluye el de acceso a los archivos, registros y documentos públicos, A*cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren...@*,y en especial A*el acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figurean incompletos o inexactos, podrán exigir que sean rectificados o completados...@* (art.37.1 y 2). Por su parte el art. 45, al hacer mención a la *incorporación de medios técnicos* (TIC) al derecho, *Acon las limitaciones que a utilización de estos medios establecen la Constitución y las leyes@* (art. 45.1), hace énfasis en la compatibilidad de esta utilización con el ejercicio de los derechos del titular (art.45.2), terminando con una denominación de documento electrónico, informático y telemático (art.45.5). Como se puede apreciar, sobre estos tópicos resulta más precisa la LRJPA que la LORTAD, cara la interpretación del Código Penal, no sólo en el título X, sino en otras partes donde repetidamente se utiliza la conceptualización técnica TIC, para proteger derechos e intereses legítimos de las personas. Por ello no han dudado los iusadministrativistas al plantear la conexidad y la observancia de *la unidad de materia* reguladas entre la LRJPA y la LORTAD [**102**], cuando está presente la informática y el derecho (la iusinformática), aunque el legislador actúa a espaldas de esa realidad temática y prefirió dejar a la doctrina que desentrañara esa sintonía.

Finalmente, la Directiva 95/46/CE, --que precisa y amplia el Convenio de Europa de 1981, sobre la materia--, en su art. 12, extiende el derecho de *habeas data* inicialmente al derecho de

(102) Véase, GONZALEZ NAVARRO, F y GONZALEZ PEREZ, J. Ob. cit., págs.686-714 y 808-854

acceso que ostentan ***todos*** los interesados para obtener del responsable del tratamiento automatizado de los datos o de la información de ciertas acciones, conductas y mecanismos de control, protección y obtención de información o consulta que le concierne, a la vez que impone unas excepciones o limitaciones a éste derecho devenidas principalmente de la seguridad del Estado, la defensa, la seguridad pública, por ser objeto de investigación penal o de infracciones deontológicas en las profesiones, por un interés económico y financiero estatal, por la protección del interesado o de los derechos y libertades de otras personas (art.13.1 Id). Los derechos del concernido; entre otros, son: a) los de confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen; la comunicación de los mismos y de su origen, así como el conocimiento de algunos tratamientos automatizados de datos, cuando se tiendan a evaluar determinados aspectos de la personalidad, como p.e., el aspecto laboral, la fiabilidad, la conducta, etc. (art. 15.1.id); b) la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, por ser incompletos o inexactos; c) Notificación a terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el anterior literal y siempre que no resulte imposible o suponga un esfuerzo desproporcionado.

5.2.2.1.2. Utilización y Alteración.

La acción de utilizar, en perjuicio de tercero o mejor del titular **[103]** de los datos o informaciones de carácter particular o familiar que se hallen registrados en documentos informáticos, electrónicos y telemáticos en archivos o registros públicos o privados, ha sido objeto

---

(103) Al respecto, se comenta que Asorprende la inclusión de un elemento subjetivo del injusto en este tipo de conducta delictiva; probablemente con esta partícula intencional el legislador ha pretendido reservar la incriminación típica para las conductas de dolo directo, excluyendo las de dolo eventual. La Expresión Atercero@ parece, en principio querer referirse al titular de los datos, pues la LORTAD tiene por Aafectado a la Apersona física titular de los datos que sean objeto de tratamiento electrónico@ (art.2.3. e) LORTAD). Sin embargo, en el segundo inciso del art. 197.2 C.P., se alude a conductas verificadas en perjuicio del Atitular de los datos o de un tercero@. Esta cláusula induce a la perplejidad puesto que la tutela del Ahabeas data@ en la LORTAD se instituye para proteger a la persona física titular de los datos, y a ésta exclusivamente debería referirse el C.P. Por ello, lo más prudente es interpretar que Atercero@, en el primer inciso del precepto es la Apersona física titular de los datos personales@. Cfr. MORALES PRATS, F. Ob. cit.pág.173. Muy a pesar de ello, la Directiva 95/46/CE, en el art. 2, f), sí distingue entre titular de los datos y el tercero. Sobre este último dice que es ALa 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@.

de tipificación doble en un mismo apartado (art. 197.2 *ab initio* C.P.Esp.), como dijimos, conduce a multitud de problemas interpretativos por no observar el ciclo operativo completo de los banco de datos en su creación (se entiende desde la recolección de los datos, con excepción de la recogida manual de que es preinformática), almacenamiento, registro y transmisión (p.e., para consulta) y sólo reducirlo al registro de los datos para encuadralo los tipos en sede penal, como sostiene el profesor *Morales Prats* [104], pero además crea una incertidumbre jurídica al tipificar *in fine* del art.197.2., nuevamente la utilización de datos sin mencionar que éstos estén o no registrados, lo cual nos llevaría a pensar que en éste aparte sí esta previsto ese ciclo o fases del ingreso o acceso, tratamiento o procesamiento y consulta automatizada de datos o informaciones de carácter particular. Y, aquí el desconcierto es mayor, pues las conductas de recogida ilícita de datos personales con fines informáticos y la creación clandestina de ficheros o bancos de datos personales con fines de automatización y manejo de datos personales, encuentran respuesta sancionadora *extra-muros* del Derecho Penal, como infracciones administrativas en la LORTAD (art. 43.4 a) y art. 43.3.a), b), y c) [105].

Una aproximación hermenéutica a la solución del problema debería comenzar sintonizando la regulación de un mismo nuevo fenómeno tecnológico, como el TIC, su regulación por parte del derecho, la visión iusformática prevista en la LORTAD, con la reglamentación del derecho de habeas data contenido en la LRJPA y su Real Decreto No. 263/1996, de 2 Febrero, al menos para comprender holísticamente los derechos de acceso, utilización y alteración de los datos o informaciones.

En la exposición de motivos de la LORTAD, se sostiene que el art 18.4, de CE, emplaza al legislador a limitar el uso de la informática para garantizar la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos, con lo cual se fija directrices y mecanismos de control y de protección que tienden Aexpresamente a la articulación de garantías *contra la posible utilización torticera de ese fenómeno* de la contemporaneidad que es la informática@ [106] en

---

(104) MORALES PRATS, *Protección a la* ... Ob. cit., págs.170-175
(105) Ibídem, pág. 171.**(106)** Exposición de Motivos de LORTAD. AA.VV. Base de datos Aranzadi S.A., Pamplona, 1997.

las fases del recolección, almacenamiento y acceso al tratamiento automatizado de datos o informaciones. Sin embargo, en el texto de la ley la utilización lícita del fenómeno informático sólo es posible gracias a la interpretación por exclusión de lo ilícito, pues el legislador precisó varias formas de infracciones administrativas (muy graves, graves y leves) de Autilización y cesión ilícita de datos de carácter particular (art.48, LORTAD), pero no la forma de utilizar lícitamente la informática como sí lo hicieron normas posteriores sin conexión sistemática alguna. Por ello, cabe el enclave interpretativo siguiente.

En efecto, la LRJPA, al reglamentar el derecho de acceso de los ciudadanos ante la administración general del Estado, prevé la incorporación de medios técnicos informáticos y/o telemáticos, la forma de acceso y utilización de los mismos, A*con las limitaciones que a la utilización de estos medios* (se refiere a los informáticos, electrónicos y telemáticos) *establecen la constitución y las leyes@ (art.45.1)*. Los límites constitucionales a observar serán los que imponen todos los derechos fundamentales (art. 10 y 55.1 CE) y los legales, los previstos en la LORTAD y la propia LRJPA. La utilización de medios informáticas y/o telemáticos, como derecho de los ciudadanos no es absoluta, pues está limitado a la Constitución y el Ordenamiento Jurídico vigente.

La ilícita utilización de los medios técnicos en estas relaciones jurídicas del ciudadano y el Estado, será sancionada por el Código Penal, y en particular, cuando el bien jurídico sea el de la intimidad y previamente se acceda a archivos, registros o do cumentos informáticos y/o telemáticos públicos y privados, según el art. 197.2.

La licitud en la utilización de los medios informáticos y/o telemáticos, está prevista en el R.D.263, de 2 de febrero de 1996 que reglamenta el art. 45 de la LRJPA, *con la pretensión de delimitar, en el ámbito de la Administración General del Estado, las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas*, como se sostiene en la exposición de motivos del referido Real Decreto. Destaca que la utilización de las técnicas señaladas tendrán las limitaciones establecidas en la Constitución, la Ley 30/92, el A*resto@* del ordenamiento Jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos. En especial, se garantizará el honor y la intimidad personal y familiar de los ciudadanos, ajustándose, a tal efecto, a lo dispuesto en la Ley Orgánica 5/1992", (LORTAD) y en las demás leyes específicas que regulan el tratamiento de la

información así como sus correspondientes normas de desarrollo. La utilización de tales técnicas en ningún caso podrá implicar la existencia de restricciones o discriminaciones de cualquier naturaleza en el acceso de los ciudadanos a la prestación de servicios públicos o a cualquier actuación o procedimiento administrativo (art. 2).

Igualmente se establecen las garantías generales de la utilización de los soportes, medios y aplicaciones electrónicas, informáticas y telemáticas (art. 4) y dentro de las medidas de seguridad que deben garantizar la administración del Estado y sus entidades de derecho público; entre otras, las siguientes: a) Cuando se utilice medios técnicos, se adoptarán medidas sinónimas y de organización necesarias que aseguren la autenticidad, la confidencialidad, integridad, disponibilidad y conservación de la información. Estas medidas deben tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos, y b) Se aplicará medidas que garanticen, la prevención de alteraciones o pérdidas de los datos e informaciones y la protección de los procesos informáticos frente a manipulaciones no autorizadas.

Esto último nos sirve para hacer énfasis sobre la *alteración de datos* y como acertadamente se sostiene por la doctrina iuspenalista, la acción de modificación es sinónima a la de alteración utilizada por el legislador en el art. 197.2. [**107**]. Esta es otra más de las inconsistencias gramaticales del mentado artículo, que conllevan a tipificar doblemente una misma acción, sin necesidad ni rigor jurídico. Por ello, a nuestros fines preferimos manejar la conducta comportamental humana de alteración por ser más explicativa en el proceso de tratamiento automatizado de datos o informaciones personales.

---

(107) MORALES PRATS. Ob. ut supra cit., pág.173

5.2.2.2. Parte *in fine* del tipo: La Interceptación o la intervención..

La acción del *delito de interceptación de los datos o informaciones de carácter personal o familiar contenidos en documentos electrónicos o telemáticos* (art. 197.1 in fine C.P.Esp.) consiste en interceptar datos con medios informáticos para descubrir la intimidad. Hay que entender por interceptar la intervención para conocer el contenido de la misma, de ahí que sólo sea punible la comisión dolosa [108]. La interceptación de los datos o informaciones de carácter particular se hacen interceptando las telecomunicaciones o teletransmisiones de datos que contengan voces (naturales y digitalizadas), sonidos, imágenes (estáticas y en movimiento) y datos alfanuméricos: textos o figuras (gráficos o digitalizados), componentes de un documentos electrónicos o telemáticos y emitidos y recepcionados por medios tecnológicos, TIC e informática. v.gr. por vía internet, por correo electrónico, La multimedia y la red alámbrica e inalámbricas de teletransmisión que une datos, imagen y texto. Obviamente se debe entender que esta interceptación delictuosa de las telecomunicaciones debe tender a descubrir la intimidad y la imagen como expresión o visión de éste (elemento subjetivo del injusto) y que excluye las infracciones administrativas de interceptación de telecomunicaciones no destinadas al uso público o a cualquier otro uso, previstas en el art. 33 de la Ley de Ordenación de las Telecomunicaciones (LOT: 31/1987, de 18 de diciembre) [109] .

Debemos partir de una premisa constitucional básica para tratar el tema, y es el de que A*se garantiza el secreto de las comunicaciones y, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial@* (art.18.3), entendiendo que en el género de las comunicaciones se halla el fenómeno tecnológico TIC y las denominadas telecomunicaciones. Por ello, A*sea cual sea el ámbito objetivo del concepto de comunicación, el art.18.3... se dirige inequívocamente a garantizar su impenetrabilidad por terceros ajenos a la comunicación; no hay secretos para aquel a quien se dirige la comunicación@* (STC 114/1984, Nov. 29). En concor-

(108) Vid. SERRANO GOMEZ, A. Ob. cit. pág. 229

(109) Sin embargo, el principio del *non bis in ídem*, entre sanciones penales y administrativas, en éste punto se halla vulnerado, al prever, entendemos, que el art. 197.1 y el art.33 de la Ley de telecomunicaciones hay regulado doblemente un misma conducta. Esto ha sido objeto de recurso de inconstitucionalidad ante el Tribunal Constitucional. SERRANO GOMEZ, A. Ob. cit. pág. 299

dancia, el art.22 LOT, expresa que se garantizará A*el secreto de las comunicaciones*@.

El bien constitucionalmente protegido, en el art.18.3 CE, con el secreto de las comunicaciones, es en términos del Tribunal constitucional la A*Libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (*que suponga aprehensión física del soporte del mensaje, con consecuencia o no del mismo o captación de otra forma del proceso de comunicación*) como por el simple conocimiento antijurídico de lo comunicado* (apertura de correspondencia ajena guardada por su destinatario, por ejemplo)@. (FJ.7 STC 114/1984). Esta libertad es otra más de las faceras del derecho a la intimidad.

Por telecomunicaciones, se entiende acudiendo a la LOT (anexo núm.3), A*toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos*@. A su vez, siguiendo el sistema de terminología técnica, que es la regla en el legislador de finales del siglo XX, podemos distinguir entre telecomunicaciones por ondas hertzianas o electromagnéticas o radioeléctricas (la radiocomunicación y la radiodifusión v.gr. radio y televisión , destinada al servicio del público en general), por cable y por satélite.

Las telecomunicaciones por cable, hace referencia al A*suministro o intercambio de información en forma de imágenes, sonidos, textos, gráficos o combinaciones de ellos, que se prestan al público en sus domicilios o dependencias de forma integrada mediante redes de cable*@ (Ley 42/1995, de 22 de diciembre). Entre sus múltiples servicios se incluye la radio y la televisión a domicilio o dependencia del interesado y previo contrato con las empresas que lo suministran **[110]**.

Las telecomunicaciones por satélite, son A*los servicios de telecomunicaciones para cuya prestación se utilizan de forma principal redes de satélite de comunicaciones*@ (v.gr. La televisión digital por satélite, D.L.1/1997 y Ley 17/1997).

(110) SERRANO GOMEZ, A. Ob. ut supra cit., pág. 163 y ss

Sin embargo, la legislación de telecomunicaciones no descansa exclusivamente en estas tres categorías, sino que a estos conceptos se superponen otras nociones que no atienden a la técnica empleada (ondas, cable o satélite), sino al tipo de actividad que se realiza. Reciben el nombre de Aservicios@, tales como: los finales (telefonía básica, telex, telegrama); los portadores (telefonía, radio, televisión); los de difusión (radio y televisión); y los de valor añadido **[111]**. En estos últimos están (telefonía móvil, teletex, telefax, burofax y el datafax) y consisten en

> A*los servicios de telecomunicación que, no siendo servicios de difusión, y utilizando como soportes servicios portadores o servicios finales de telecomunicación, añaden otras facilidades al servicio de soporte o satisfacen nuevas necesidades específicas de telecomunicación como, entre otras, acceder a información almacenada, enviar información o realizar el tratamiento, depósito o recuperación de información@* (art. 20.1 LOT)

Las telecomunicaciones unidas a la informática forman esa compleja amalgama que bien podríamos llamar la teleinformática y la telemática como especie de ésta. Quizá por ello, la Directiva 95/46/CE, hace énfasis sobre los objetivos y finalidades de la *Transferencia de datos personales a países terceros* (art. 25), los mecanismos de protección de los derechos y libertades que deben observarse, así como los medios tecnológicos TIC, unidos a la informática, por los cuales se transmiten, emiten y recepcionan. En efecto, cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico, y tenga éste único fin, será responsable del tratamiento de los datos personales contenidos en el mensaje, el emisor y no quien ofrezca el servicio de transmisión; *que no obstante, las personas que ofrezcan estos servicios normalmente serán considerados responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio* (C. 47).

Ahora bien, el delito que comentamos ahora, sólo requiere para su consumación el efectivo descubrimiento de la intimidad, bastando así para la perfección típica con la

interceptación de las telecomunicaciones o con la utilización de aparatos de escucha, grabación o reproducción del sonido o de la imagen o A*cualquier otra señal de comunicación*@ (p.e. la correspondencia informática que posibilita la conexión de la red telefónica al ordenador, como el correo electrónico

---

(111) Vid. CHINCHILLA MARTIN, Carmen. *El régimen jurídico de las telecomunicaciones. Introducción.. En:* Revista de la Escuela Judicial. C.G.P.J., Ordenación de las telecomunicaciones. No. VI, 1997, Madrid, pág. 12.

--*E-Mail*-- y las variadas formas de comunicación electrónica de hoy en día, tales como*: list servs, newgroups, chat rooms, y World Wide Web --WWW--;* entre otros). Estos aparatos utilizados para el control auditivo o visual, dado el carácter penetrante y permanente que estos medios facilitan en la intimidad de las personas, comportará normalmente ya el efectivo descubrimiento de aquella, según lo sostiene el profesor *Morales Prats,* al ubicar esta modalidad típica de interceptación de datos informáticos y/o telemáticos, como de *control auditivo y visual clandestino y de control ilícito de señales de comunicación de carácter informático* **[112]**., y con esto último, se establece una cláusula abierta que permite ofrecer una cobertura típica amplia a cualquier modalidad, tipo o servicio de comunicaciones **[113]**, tanto tradicional como actual (p.e. la telemática: multimedia y la hipermedia).

Un aspecto importante a destacar en esta figura típica de la interceptación de datos o informaciones de carácter personal, es que para su configuración se requiere que no haya consentimiento del sujeto pasivo del delito, o de todos, si son varios los que intervienen en una comunicación, pues de lo contrario la tipicidad se excluye, como lo han expuesto *Serrano Gómez, Muñoz Conde* y desde antes del C.P de 1995, *Bustos Ramírez* **[114]** o se cae en otro tipo penal, pero no en éste. Sin embargo, se ha estimado que la alusión de la norma penal (art.197.1) a A*sin su consentimiento*@ (del titular se entiende), en términos de la LORTAD, debe referirse a una A*ausencia de consentimiento del titular de los datos*@, y por tanto, el C.P. de 1995 debería haber indicado que esas conductas deben realizarse *ilegalmente* **[115]** y así evitar la alusión que hoy trae en forma expresa, pues tácitamente puede entenderse que no ha habido consentimiento por parte del titular y que las conductas que se realizan no han tomado en cuenta su consentimiento. Aunque es pleonástico decir que la conducta se realiza ilegalmente, pues ello va inmerso en el concepto delito, referido en el art. 197 *in fine*, que resulta más apropiado que el de la frase de cajón: sin su consentimiento, entendido sólo en forma expresa.

---

(112) Ibídem, pág. 15 y ss. No es sólo son los E-Mail, sino mediante una variada gama como se ejerce ese control.
(113) MORALES PRATS, F. *Comentarios a la parte...* Ob. cit., pág. 304.
(114) Vid. Ob. ut supra cits. págs. 229-230; 220-221; y , 94, respectivamente.
(115) Ibídem., págs. 172.

Quizá por esto, el Código Penal Canadiense, en el art. 193.1(1) a), tipifica en forma autónoma el delito de *Disclosure of information received from interception of radio-based telephone comunications* y cuando estas comunicaciones sean interceptadas por medios electromagnéticos, acústicos o mecánicos o cualesquiera otros, sin el consentimiento expreso o tácito del titular o de las personas involucradas en la comunicación, para evitar la interpretación sobre el consentimiento tácito, antes mencionado.

Ahora bien, con igual criterio al observado en el aparte anterior (b), utilización y alteración), como enclave de interpretación normativa de LORTAD y LRJPA, respecto al entendimiento del fenómeno ilícito de la interceptación de datos informáticos previsto en el art. 197.1. *in fine*, debemos recurrir a la lícita reglamentación de la utilización de técnicas electrónicas, informáticas y telemáticas por la administración General del Estado, estipulada en el R.D. 263/1996, de 16 de Febrero, art. 7.

> *Comunicaciones en soportes o a través de medios o aplicaciones informáticos, electrónicos o telemáticos.* ***1****. La transmisión o recepción de comunicaciones entre órganos o entidades del ámbito de la Administración General del Estado o entre éstos y cualquier persona física o jurídica podrá realizarse a través de soportes, medios y aplicaciones informáticos, electrónicos y telemáticos, siempre que cumplan los siguientes requisitos:* ***a)*** *La garantía de su disponibilidad y acceso en las condiciones que en cada caso se establezcan.* ***b)*** *La existencia de compatibilidad entre los utilizados por el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseños de registro establecidos por la Administración General del Estado.* ***c)*** *La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados.* ***2.*** *Las comunicaciones y notificaciones efectuadas en los soportes o a través de los medios y aplicaciones referidos en el apartado anterior serán válidas siempre que:* ***a)*** *Exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones.* ***b)*** *Se identifique fidedignamente al remitente y al destinatario de la comunicación.* ***c)*** *En los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos hayan señalado el soporte, medio o aplicación como preferente para sus comunicaciones con la Administración General del Estado en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa.* ***3.*** *En las actuaciones o procedimientos que se desarrollen íntegramente en soportes electrónicos, informáticos y telemáticos, en los que se produzcan comunicaciones caracterizadas por su regularidad, número y volumen entre órganos y entidades del ámbito de la Administración General del Estado y determinadas personas físicas o jurídicas, éstas comunicarán la forma y código de accesos a sus sistemas de comunicación. Dichos sistemas se entenderán señalados con carácter general como*

preferentes para la recepción y transmisión de comunicaciones y notificaciones en las actuaciones a que se refiere este apartado. ***4.*** *(...)*@

Una reciente sentencia del Tribunal Constitucional, como lo destaca *Queralt Jiménez* [116], con motivo de la reforma operada por la LO 18/1984, tenía por objeto proteger la inter-

---

(116) QUERALT JIMENEZ, J.J. *Derecho penal Español. Parte Especial, 3 ed.* Ed. J.M. Bosch, Barcelona, 1996, pág. 195

ceptación, no sólo de las conversaciones telefónicas strictu sensu o conversacionales, sino cualquier tipo de telecomunicación. Así se terminó con la duda que asaltaba a algunos al entender si estaban o no previstas otras formas de comunicación como el fax o la telefonía celular, y creemos nosotros, que cualquiera otro medio de comunicación que una telecomunicaciones e informática (telemática, vía internet, correo electrónico, etc.), como antes indicábamos. En consecuencia, cualquier A*captación y divulgación de las conversaciones telefónicas, sea cual sea el sistema que utilicen los interlocutores es ilícita*@, entendiendo que interceptar en los términos de la sentencia, consiste en *apoderarse del mensaje antes de que llegue a su destino o interrumpir una vía de comunicación.* (STC 34/1996, de 11 de marzo. Aunque como se sabe ésta se refiere a la interceptación de comunicaciones por funcionarios o agentes públicos --art. 536 C.P.--, pero en todo caso contra la intimidad de las personas).

En esta última línea y fin, y con motivo de la noticia de la intervención, acordada por un juez norteamericano, respecto de las comunicaciones que circulan por las redes informáticas, vía internet y con el propósito de la investigación de unos hechos presuntamente delictivos, *Maza Martín* [117], sostiene que dicha intervención debe ser asimilada en el derecho español, en sus efectos procesales, a la telefónica, así como los requisitos para su eficacia probatoria. Estos serán: a) la autorización de su realización por autoridad judicial en resolución motivada; b) el carácter excepcional y por tiempo determinado; c) el que se dirijan a la obtención de pruebas sobre un hecho delictivo concreto de que consten los indicios de su comisión; d) practicada sólo sobre teléfonos de personas sospechosas de participar en los delitos investigados y llevadas a cabo bajo riguroso control del juez autorizante; y e) con la obligación de entrega a la autoridad judicial de los soportes originales en que se haya recogido el contenido de las intervenciones (STS, de 24 de Junio de 1995). El Tribunal Supremo Español, Sala 20, tiene una amplia como fecunda jurisprudencia sobre las Aintervenciones telefónicas@ (o A*escuchas telefónicas clandestinas*@ como vulgarmente se les conoce) v.gr. un resumen fructíferamente sobre el tema: Marzo 2 de 1996 (M.P. Montero Fernández Zapater), Octubre 26 de 1996 (M.P. Bacigalupo Zapater) y la de Diciembre 17 de 1996

---

(117) Citado por PEREZ VALLEJO, Ana M. *La informática y el derecho penal*. En: Actualidad Informática Aranzadi. Ed. Aranzadi, Pamplona (Esp.), No. 19, Abril, 1996, pág. 10.

(M.P.Martínez-Pereda Rodríguez).

Pero, hay más: la compleja amalgama que conforma la tecnología TIC, las telecomunicaciones y la informática; por un lado, avanza día por día, en ese también complejo como ambiguo marco de mejoras potenciales de las nuevas tecnologías en la sociedad de la informática; y por otro, los constantes, penetrantes y porosos riesgos que éstos avances representan frente a los derechos fundamentales de la persona, principalmente del derecho a la información, expresión, la intimidad y el honor. Así mismo, son constantes las dificultades de todo tipo y cada vez mayores las garantías reales y medios de protección, por parte del Estado para prevenir, evitar, o más aún, reprimirlos civil, administrativa o penalmente.

Una reciente Sentencia de la Corte de Apelaciones de los Estados Unidos de América, de Octubre 31 de 1994, conocido como el caso *Steve Jackson Games, Inc. et al. v. US Secret Service* **[118]**, se hizo referencia, entre otros aspectos, a los que llamamos medios comisivos informáticos (de hardware y software) de conductas ilícitas y de los que nos ocuparemos más adelante; y sobre todo, el diferente tratamiento jurídico devenido de la tecnología aplicada a una y otra forma de comunicación (la llamada en la sentencia Comunicación por A Cable@-- *Wire*-- y la comunicación Aelectrónica@), el tiempo en el que se realiza la intervención o interceptación (factor temporal), la variada forma de almacenamiento de la información o datos (en forma electrónica solo para la comunicación ídem, mediante software o hardware: discos fijos y removibles) y en fin, el trami-

---

(118) En el caso norteamericano que tiene por fundamento la incautación por los Servicios Secretos de los Estados Unidos, de medios informáticos físicos o de hardware (ordenador con su unidad central de procesamiento CPU y unidades periféricas) y lógicos o de software (programas de ordenador), por presunta comisión de actos ilícitos de un colaborador de un sistema electrónicos de tablón de anuncios (*AElectronic Bulletin board system@.BBS)* con información y negocios específicos de libros y publicaciones. El sistema BBS, contenían mensajes privados de correo electrónico enviados por personas interesadas en la información y negocios. Estos se almacenaban en la memoria del disco duro del ordenador como copia de seguridad o *(backup)*. Los mensajes se almacenaban, pero no alcanzaron a ser leídos por el destinatario cuando fueron incautadas por el *Secret Service US* . Steve Jackson Games, Inc et all, como demandante, sostenían que el actuar de la Agencia Especial de EE.UU, constituía una intervención o interceptación ilegal de las comunicaciones electrónicas, en virtud de la Ley Federal de Comunicaciones por Cable. 18 U.S.C., enmendada por la Ley de Protección a la intimidad en las comunicaciones electrónicas de 1986 (*The Electronic Communication Privacy Act of 1986*). La Sentencia, estimó que en el caso presente no existió interceptación de comunicación electrónica, almacenada en disco y backup, pero no leída. El texto completo de la Sentencia de la Corte de Apelaciones de los Estados Unidos de América, 51 Circuito, Octubre 31 de 1994, Caso Steve Jackson v. Secret Service US. En: *WWW.UMONTREAL.CA. (Universidad de Montreal Canadá).*

te distinto seguido por parte de las autoridades judiciales y/o administrativas, para la interceptación de comunicaciones electrónicas (*electronic communication*) y la intervención de comunicaciones por cable (*Wire communications*). Aunque, queda claro que tanto una y otra forma de comunicación son objeto de interceptación, pues la *intercepte*, se define como *Aadquisición auditiva o similar de cierto volumen de información o comunicación por cable, electrónica, o en forma oral, a través del uso de cualquier dispositivo electrónico, mecánico u otros@,* según el art. 2510 del Act Wiretap, 18 U.S.C. La interceptación, requiere un elemento temporal fundamental para que ésta se cumpla . En efecto, *A...la adquisición* (debe ser) *contemporánea a la comunicación* (es decir, a la transmisión: emisión y recepción del mensaje), *a través del uso del dispositivo@* idóneo (instrumentos y/o aparatos TIC e informática) según se trate de comunicación por cable o electrónica y que en éste último caso, la información no esté almacenada o guardada en memoria o discos de computador

En efecto, se dijo que la *comunicación electrónica,* se define como*: cualquier transferencia de señales, signos, escritura, imágenes, sonido, datos o informaciones de cualquier naturaleza transmitidas en todo o en parte por cable, radio o en forma electromagnética, foto-eléctrica o por sistema foto-óptico y afectan al comercio entre estados o con el extranjero.*(F.N.4 de la Sent. C.F.US. Oct.31/94).

No queda cubierta en esta definición las comunicaciones siguientes: a) La realizada mediante radio-teléfonos o los teléfonos inalámbricos, ni la comunicación entre éstos con unidades de teléfono fijas; b) Cualquier comunicación por cable en forma oral; c) Cualquier comunicación realizada, a través de sólo tonos con dispositivo de paginación; y, d) Cualquier comunicación realizada con un dispositivo de rastreo, definidos en el artículo 3117 de la Ley Federal de Comunicaciones por Cable (*The Federal Wiretap Act, 18 U.S.C*) (FN.4 *In fine*). Enmendada por la Ley de Protección a la intimidad en las comunicaciones electrónicas de 1986 (*The Electronic Communication Privacy Act of 1986.*

Los mensajes de correo electrónico (*E-Mail*) [119], fueron el objeto de la supuesta intervención o interceptación de las comunicaciones electrónicas, en el caso norteamericano, por cuanto los Servicios Secretos de los Estados Unidos (*Secret Service US*), incautaron un ordenador, con sus programas, unidades de almacenamiento (*storage*) de la información o datos, tanto principal (Disco Fijo o Duro), como de copias de seguridad (*Backup*) --formas exclusivas de la comunicación electrónica--, con motivo de una investigación preliminar, por supuesta comisión de un ilícito por parte de uno de los colaboradores y/o trabajadores de una empresa particular que laboraba con el Sistema Electrónico del Tablón de Anuncios (BBS), en el cual se almacenaba la información enviada por los destinatarios mediante los *E-Mail privados,* no leídos por el destinatario *Steve Jackson Games Inc*., antes de la incautación.

La Corte de Apelaciones, estimó que siendo distinto los sistemas de comunicación por cable (*Wire*), y los de comunicación electrónica, como la realizada por mensajes de correo electrónico, se deberá diferenciar en ésta última, sí: a) las comunicaciones electrónicas han estado en almacenamiento electrónico (en discos fijos y removibles o unidades de copia de seguridad) durante 180 días o menos, el gobierno puede acceder a su contenido, sí dispone de una *garantía federal o estatal* (*Federal or state warrant*), a términos del art. 2703 de la Act Wiretap , 18 U.S.C.; y, b) si las comunicaciones que son almacenadas por un servicio remoto de informática

---

(119) *Los mensajes de correo electrónico* (E-Mail), son una de las variadas formas típicas de comunicación electrónica de hoy en día y tiene por objeto, comunicar o transferir datos o informaciones de todo tipo y naturaleza (texto, imagen o sonido), entre dos personas, a través de ordenadores o computadores ubicados en diferentes lugares del planeta. Para ello deben disponer de una línea telefónica, un *MODEM* (Modulador y DEModulador de señales), un operador de comunicaciones (como Telefónica en España, Telecom en Colombia), un proveedor de acceso a la información (como SIEMENS) y un proveedor de contenidos de la información (particulares o instituciones públicas o privadas. p.e. Universidades). En el punto, 5.5.5.2., volveremos sobre el tema y sobre la sentencia de la Corte.. *Sin embargo, adelantemos que hoy en día cualquier persona, puede enviar y recibir un E-Mail, como ayer (siglos atrás), lo hacía, a través de una carta escrita.* Las facilidades de comunicación electrónica a través de E-Mail, como de otros mecanismos de comunicación electrónica (v.gr. Los foros de debate --Newgroups--), han posibilitado un avance significativo y democrático de las comunicaciones a todo nivel y en cualquier sitio del planeta. Paradójicamente esa facilidad en el acceso, consulta y de disposición de equipos y aparatos informático aptos para la comunicación engendra un sinnúmero de formas violatorias de derechos humanos, los cuales plantean nuevos retos y soluciones para los juristas que deben empezar por comprender el fenómeno tecnológico TIC en matrimonio --si nos permiten-- con la informática. Sólo así podremos entender la conducta humana y las actividades de las personas que ya no utilizan una arma física, sino una especie de arma físico-lógica, como el ordenador o computador conectado, vía telefónica a través de un modem, un operador de telecomunicaciones con otro para cometer atentados contra los derechos fundamentales, patrimoniales o no patrimoniales. *El delito de finales del siglo XX y principios del siglo XXI, se caracteriza por la notable sutileza, muchas veces anónima, con que se utilizan los medios físico-lógicos (hardware y software) en la comisión de una conducta ilícita.*

(*remote computing service*) y ésta ha permanecido por más de 180 días, el gobierno puede acceder a su contenido, siempre que disponga una garantía por vía administrativa del Gran Jurado o haya obtenido una orden judicial de la Corte, a tenor del artículo 2703 Ibídem.

5.2.3. Los Adatos sensibles@ de la persona humana.

5.2.3.1. Información personal del concernido.

Los datos de carácter personal se han considerado como A*cualquier información concerniente a personas físicas, identificadas o identificables*@ (art.3, a, LORTAD). A su vez persona identificable es aquella a quien puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social (art.2,a), Directiva 95/46/CE). La persona identificable también se le denomina A*interesado*@ o impropiamente A*afectado*@, según la LORTAD, pues destaca el aspecto negativo del derecho que tiene una persona humana (v.gr. la vulnerabilidad) y no el positivo de ser titular de los mismos o tener interés legítimo para ejercitarlos en las condiciones previstas en la Constitución y el ordenamiento jurídico vigente.

En términos iusinformáticos, las expresiones A*cualquier información*@, deben interpretarse como una unidad de datos (textual, imagen o sonido) representada en forma binaria (0/1) en el tratamiento computarizado y relacionado con una persona natural o física. La información recogida, procesada, almacenada y recuperada por consulta o transferencia total o parcialmente por medios Aautomáticos@ y electrocomputacionales. Esta información se caracteriza por ser relevante, clara, oportuna y confiable. Relevante significa que el contenido transmitido es por sí solo suficiente para ser comprendido por el receptor de una información. Clara e inteligible significa que sea transparente, de fácil entendimiento y que el mensaje transmitido por el emisor sea través de canales aceptables y entendibles para el receptor. La oportunidad hace relación a la temporalidad en la que es transmitida y recepcionada; y finalmente confiable, significa que reúne todos los elementos y calidades anteriores [120]. Sin embargo, se ha creído que el término *cualquier*

---

(120) Vid. Mi trabajo, *La Constitución*... Ob. cit. pág. 7 y ss.

información utilizado por la LORTAD constituye un error de definición consistente en no haber excluido de su ámbito objetivo a un núcleo mínimo de datos, para así evitar que toda información relativa a una persona física, por nimia que parezca, constituya un dato de carácter personal a los efectos legales [121].

Pero lo que no se repara es que la información de carácter personal a la que hace referencia la LORTAD, es la referida al concernido dentro de un marco constitucional de derechos y libertades inherentes a la persona humana (arts. 14,15,16 y 55.1 CE), valores y principios como la dignidad de la persona, el desarrollo de la personalidad, el interés público, la paz social y democrática (art. 10 CE); y los límites constitucionales a los derechos de los demás previstos en la propia CE (art. 18.4., 20.1.d) y la ley (LORTAD y normas de desarrollo).

Por contra, para quienes reclaman más excepciones y limitaciones al concepto A*cualquier información*@; además y, por si fuera poco, se sostiene que la LORTAD, paralelo al cúmulo de derechos (principalmente integrantes del *habeas data),* se plantea una escalonada y categórica relación de excepciones y limitaciones establecidas para los titulares de los datos, los ficheros de titularidad pública y privada (aunque sean más acusadas para los de carácter público), que no está lejos de desvirtuar los derechos constitucionales, principalmente la intimidad y el habeas data que pretende protegérselos, y quizá por ello, no se duda en calificar la actividad legislativa de los creadores de la LORTAD como una página de protección de derechos fundamentales frente a un catálogo que contiene un A*máximo de euforia de excepciones y limitaciones@,* según *Davara* y que Aafectan el contenido esencial de la garantía reconocida en el art.18.4" CE, a tal punto que ha sido_____

(121) Esto nos conduce a pensar que una Asimple agenda informática de teléfonos es un fichero de datos de carácter personal, que debe ser notificado a la APD (se refiere a la AAgencia de Protección de Datos Española@) antes de su uso, a cuyo fichero hay que dotar de sistemas de seguridad adecuados, con la obligación de informar al afectado de que integramos su teléfono a un fichero automatizado, etc @ En otro lugar, con igual intención alude: ADebemos recabar un consentimiento escrito de nuestros clientes si precisamos tener datos sobre su ideología o creencias, salud o cuestiones relativas a la vida sexual, lo cual no es inusitado en nuestra profesión, en particular por parte de los abogados matrimonialistas o penalistas (art.7, núm. 2 y 3)@. Cfr. JIMENEZ ESCOBAR, Raúl. ***Sobre la aplicación de la Ley orgánica 5 de 1992 a los ficheros automatizados de datos de carácter personal mantenidos por los abogados.*** En: Revista Jurídica de Cataluña No. 1, Barcelona, 1995, pág. 37 y 43

objeto de recursos de inconstitucionalidad ante el Tribunal Español, [122] y con fundadas razones jurídicas, como se observó en la parte primera de éste trabajo.

Este régimen de excepciones y limitaciones a los derechos, tanto en el Convenio Europeo de 1981, como en la Directiva 95/46/CE, es igualmente amplio y enfático cuando se refiere a los asuntos de seguridad y salubridad públicas, la defensa, los intereses económicos o financiero y de investigación del Estado; entre otros (art.13 y 26), y muy puntual cuando se relaciona con el régimen de protección de derechos y libertades de la persona (*intimidad* o *vida privada* y habeas data, art. 13 *in fine* y 26.2 y 3*),* todos los cuales se justifican y legitiman *por razones de seguridad del Estado o de la defensa* (C. 43).

En otras latitudes, como la canadiense, por ejemplo, han preferido no utilizar el concepto genérico de datos o informaciones personales, sino una relación de los que se consideran como tales, y aunque es una relación *numerus clausus,* la interpretación hermenéutica posibilita la actualización del listado. La *Act Privacy* canadiense [123], previamente entiende como *personal information,* la concerniente a una persona, cualquiera sean los mecanismos o tecnologías de las que se obtengan o graben, para luego relatar los siguientes supuestos de información personal:

a) La información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona. b) la información relacionada con la educación, el historial médico, delictivo, laboral de la persona, o la información relacionada a las transacciones financieras en las que el individuo ha estado involucrado. c) cualquier número o símbolo que identifique o se le asigne a una persona. d) la dirección, las huellas digitales o el tipo sanguíneo de la persona. e) las opiniones o ideas personales, excepto aquellas vertidas sobre otra persona, o sobre una propuesta de subvención, recompensa o un premio otorgado por una institución gubernamental, _____

(122) Vid. CASTELLS ARTECHE, José Manuel. *Derecho a la privacidad y procesos informáticos: Análisis de la ley orgánica 5/1992, de 29 de octubre (LORTAD).* En: Revista Vasca de administración pública., R.V.A.P. No. 39, Bilbao, 1994, pág. 268.
(123) Cfr. AA.VV. *Banco de Datos. Biblioteca Virtual de la Univ. de Montreal Canadá (versión en inglés y en francés).* WWW.UMONTREAL.EDU.CA.. Ob. cit., 1998.

sección, departamento o Ministerio, según lo estipulen sus reglamentos. f) la correspondencia enviada a una institución gubernamental por una persona que es implícita o explícitamente de naturaleza privada o confidencial, así como las contestaciones a la misma en la medida que revelen un contenido que corresponda a la envida originalmente. g) las ideas u opiniones de otra persona sobre él. h) las ideas u opiniones de otra persona sobre una propuesta de subvención, recompensa o premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos y referida en el parágrafo (e), pero excluyendo el nombre de la otra persona sobre la cual dedicó sus ideas u opiniones. i) el nombre de la persona que aparece relacionada con otra información personal y que el sólo descubrimiento del verdadero nombre revelaría información sobre aquél; pero para los propósitos de artículos 7, 8 y 26 de ésta ley y el artículo 19 de la LAIC (Ley de acceso a la información canadiense. *Access to information Act* [124]), la información personal queda excluida. J) la información de una persona que es o fue funcionario o empleado de una institución gubernamental y relacionada con la posición o funciones del mismo. Esta información incluye: 1. el hecho de que el individuo es o era funcionario o empleado de la institución gubernamental; 2. el título, dirección comercial y número del teléfono de la persona; 3. la clasificación, rango y monto del sueldo y atribuciones según su cargo; 4. el nombre de la persona que figura en un documento preparado por éste en el ejercicio de su empleo; y, 5. las ideas u opiniones personales expresadas en el curso de su empleo. k) la información sobre una persona que desempeña o desempeñó los servicios bajo contrato con una institución gubernamental. Esta información incluye: los términos del contrato, el nombre del individuo y las opiniones o ideas expresadas en el transcurso del mismo. l) información relacionada con cualquier beneficio discrecional de naturaleza financiera, incluida la concesión de una licencia o permiso, así como nominación del mismo, el nombre de quien la confirió y la naturaleza precisa

---

(124) Cfr. SECTION 6. Request for access to record. 6. A request for access to a record under this Act shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution with a reasonable effort to identify the record. SECTION 7. Notice where access requested. 7. Where access to a record is requested under this Act, the head of the government institution to which the request is made shall, subject to sections 8, 9 and 11, within thirty days after the request is received, (a)_give written notice to the person who made the request as to whether or not access to the record or a part thereof will be given; and (b)_if access is to be given, give the person who made the request access to the record or part thereof. SECTION 19. Personal information. 19.1._Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in section 3 of the Privacy Act.- 19.2. Where disclosure authorized._The head of a government institution may disclose any record requested under this Act that contains personal information if (a)_the individual to whom it relates consents to the disclosure; (b)_the information is publicly available; or (c)_the disclosure is in accordance with section 8 of the Privacy Act. Ob.cit., 1998. Texto completo en WWW.UMONTREAL.EDU.CA.

de la misma.; y, m) la información sobre una persona muerta y hasta por veinte (20) años.

La regla general para la protección de *toda información personal* en el derecho canadiense es el no descubrimiento o divulgación de los datos o las informaciones de carácter personal cuando no haya consentimiento de una persona a quien concierne una información catalogada de personal (art.3,b),) y siempre que ésta se halle bajo el control o responsabilidad de una institución gubernamental. La excepción, es que se podrá descubrir la información previo un procedimiento administrativo breve y sumario en las trece situaciones previstas en el art.8.2. de la *Act Privacy*.[125] [Mackenzie vs. Canadá (Ministerio de Salud Nacional y Bienestar Social). 1994.Primera Instancia. Corte Federal Canadiense .F.C.TD.] .Estas que se pueden catalogar de excepciones al descubrimiento o divulgación de la información por parte de un organismo del Estado, tienen como fundamento la realización de algunos de los fines de un Estado de derecho, tales como la seguridad, la defensa, la salubridad y la economía públicas, o bien los intereses generales, públicos,

(125) Artículo 8. LPDIC. *Descubrimiento (o divulgación) de la información personal*.8. (1) Una institución gubernamental bajo la cual está el control de una información personal no podrá descubrirla sin el consentimiento del concernido, salvo que se realice de conformidad con el presente artículo.(2) Cuándo se puede descubrir una información personal. (2) Sin perjuicio de lo estipulado en otras leyes, podrá descubrirse la información personal bajo el control de una institución gubernamental en los siguientes casos: a) cuando el propósito de la obtención o la compilación de la información lo determinó la institución; b) cuando se autoricen de conforme a las leyes federales o reglamentos vigentes; c) cuando sea exigido por una *citación*, orden o mandato de la corte, o cuando sea exigido por una persona u organismo con jurisdicción para compeler la producción de información , o con el propósito de cumplir un procedimiento sobre la producción de información personal ordenada por la Corte; d) cuando la información sea utilizada en procedimientos judiciales por parte del Abogado General del Canadá, en los que se vean involucrada en derecho, la Corona o el Gobierno del Canadá; e) cuando la información sea requerida por un organismo investigador del Estado y en la demanda escrita se ha precisado los propósitos del descubrimiento de la información y los fines de la investigación de conformidad con la leyes federales y provinciales; f) con el propósito de adelantar una investigación legal y en cumplimiento de un Acuerdo o Convenio entre el Gobierno y sus diversos organismos, una provincia, o entre éstos y un Estado Extranjero, o entre un organismo internacional del Estado y el Gobierno o sus organismos; g) por comunicación de un miembro del Parlamento con el propósito de ayudar a una persona a quien concierne la información a resolver un problema; h) por comunicación de la Oficina del Contralor General enviada a una persona o un organismo del Estado con el propósito de realizar una verificación del personal o auditoria contable interna; i) con propósito archivístico a los Archivos Nacionales de Canadá; j) por comunicación a cualquier persona o organismo, con los propósitos de investigación o fines estadísticos , siempre que se realicen cumpliendo estas dos condiciones: 1. que el responsable de la institución este convencido de los fines para los cuales se solicita la información y al proceder de esta forma permitirá que no se identifique al individuo concernido, y 2. obtener de la persona u organismo una constancia escrita de que no se hará ningún descubrimiento subsecuente de la información de forma tal que podría esperarse razonablemente se

identifique a la persona concernida; k) por comunicación a una asociación de aborígenes, Banda indiana, institución gubernamental, parte de éstas, o su representante, con el propósito de investigar una solicitud, disputa o agravio contra las gentes aborígenes de Canadá; l) por comunicación a una institución gubernamental con el propósito de localizar a un deudor o acreedor de la Corona del Canada para hacer efectivo el cobro o su pago; m) por comunicación del responsable de una institución gubernamental para cualquier otro propósito en cual se involucre: 1. el interés público sobre el particular que eventualmente justifique la invasión de la intimidad con el descubrimiento de una información personal, o 2. que el descubrimiento beneficie al concernido. Texto Completo en WWW.UMONTREAL.EDU.CA.

de relaciones internacionales, investigativos (judiciales o administrativos), científicos o archivísticos o, en últimas, los del concernido o interesado con la información.

5.2.3.2. Diferentes grados de protección de los datos o informaciones personales del concernido. Especial referencia al consentimiento.

La LORTAD, reconoce ciertos grados de protección a los datos o informaciones de carácter personal, de conformidad con los criterios observados en el tratamiento automatizado de la información y, sobre todo, del consentimiento de la persona concernida, que bien puede sostener y representarse en una tipología de los datos de ultraprotección, datos de protección calificada y los datos de protección general, como en seguida veremos.

Sea lo primero decir que, tratamiento automatizado, es el conjunto de operaciones y procedimientos técnicos de carácter automatizado que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como la cesión de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (art. 3,c), LORTAD). Definición que en esencia es igual a la observada por la Ley núm. 78-17, de 6 de enero de 1978, *relativa a la informática, los ficheros y las libertades.*, el Convenio de Europa de 28/1/81, art. 2., c), ratificado por España el 27 de Enero de 1984 y la Directiva 95/46/CE, art.2, b),relativa a la protección de las personas físicas en lo respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Esta definición como las fases del tratamiento automatizado de los datos de carácter personal previstas en ésta, por la ubicación, el contenido y los criterios orientativos y hermenéuticos que tiene en la LORTAD, se aplica a toda clase de datos en ésta previstos y sin perjuicio de que se haga énfasis para una cualquiera de las fases o del ciclo de tratamiento informático y su correspondiente régimen de protección reforzado. v.gr. el art. 7.3. LORTAD.

La regla general es que el consentimiento de la persona concernida se requerirá siempre para el tratamiento automatizado de los datos personales, salvo que la ley disponga lo contrario o que pueda ser revocado por causa justificada y sin efectos retroactivos o *ex nunc* (art.6.1 y 3).

Las excepciones a la regla se presentan en los siguientes eventos: a) cuando los datos se recojan de fuentes accesibles al público, b) cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, c) cuando se refieran a personas vinculadas por una relación negocial, laboral o administrativa, o un contrato y sean necesarias para el mantenimiento de las relaciones o para el complimiento del contrato.

Con éstas premisas, los datos de carácter personal a tenor de la LORTAD, serán de ultraprotección, sí se requiere el consentimiento expreso y escrito de la persona concernida para el tratamiento de automatizado de los datos que revelen la ideología, religión y creencias (art.7.2 LORTAD y 16.2 CE).

De protección calificada, si se requiere el consentimiento expreso de la persona concernida para el Atratamiento automatizado y cesión@ de datos de carácter personal que hacen referencia al origen racial, a la salud y a la vida sexual, siempre que sea por razones de interés general previstos en la ley, es decir, por *habilitación legal expresa*, según la exposición de motivos de la propia LORTAD. (art. 7.3 LORTAD).

Algunos de los mecanismos de protección para los anteriores datos se refleja en la prohibición a la creación de ficheros con finalidad exclusiva de almacenar datos de carácter personal que revelen ideología, religión, creencias, origen racial o vida sexual (7.4. LORTAD). En cuanto a los datos de carácter personal relativos a la salud de las personas, sólo podrán procederse al tratamiento automatizado o la cesión de datos prevista en el art. 11 LORTAD (para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario), por parte de las instituciones y centros sanitarios públicos o privados y los profesionales correspondientes, de conformidad con las normas especiales (Ley 14/1986, de 25 de abril, General de Sanidad; Ley 25 de 1990, de 20 de diciembre, del Medicamento; Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás leyes sanitarias), previo el consentimiento del concernido.

En cuanto a los datos de carácter particular relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Estas prohibiciones, restricciones y limitantes al tratamiento automatizado de los datos relativos al 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, previstas en la Directiva 95/46/CE, art.8.1. ACategorías especiales de tratamientos@, desde el Convenio Europeo de 1981, en su art. 6, ya habían sido detectadas bajo el epígrafe de ACategorías particulares de datos@, en las cuales se incluye los datos de carácter personal referentes a condenas penales y no se incluye los datos referentes a la pertenencia a sindicatos relacionada en la Directiva. (por las claras razones no sólo temporales de la norma sino por el impacto social, gremial, político y de poder de la información actual sobre el tema, aunque la Ley francesa sobre la informática ya la preveía). A pesar de las prohibiciones al tratamiento automática estipuladas en el Convenio, se deja abierta la posibilidad para que puedan hacerlo los Estados en su Aderecho interno@, siempre que se Aprevea garantías apropiadas@. La Directiva aparentemente fue más tajante al prohibir cualquier tratamiento de datos personales, sin cláusulas abiertas. Sin embargo, bajo el amplio pero puntual régimen de excepciones y las desnaturalizaciones o derogaciones de la regla general de prohibición previstas en la Directiva, no sólo es posible regular sobre la temática prohibida sino que se tienen parámetros en cascada para hacerlo en el art. 8.2 [a), a e),], 8.3. a 8.7., aparte claro está ,de las no aplicaciones de la regla general en cada etapa o fase del ciclo de tratamiento automatizado que también es amplio. v.gr. art. 13 de la Directiva.

Por exclusión de los A*datos especialmente protegidos*@ en el art. 7 de la LORTAD, se presentan los datos de carácter general con régimen de protección y tratamiento automatizado general, es decir, se aplicará la regla general del consentimiento y las excepciones, sin más.

Con base en el criterio o principio del consentimiento o de A*autodeterminación*@ como lo denomina la exposición de motivos de la LORTAD, la doctrina española [126], ha clasificado a los datos de carácter personal, así: a) datos de carácter general, y b) datos Asensibles@(término también utilizado por la exposición de motivos de la LORTAD, para destacar el nivel reforzado de protección) o Ahipersensibles@, contraponiendo un tratamiento y régimen de protección, que sólo se funda en el consentimiento del afectado, salvo que la ley disponga otra cosa, para los primeros; al de los datos sensibles o Ahipersensibles@, cuyo consentimiento debe ser por escrito y expreso, del afectado al cual deberá advertirse de su derecho a no prestarlo. Por su parte, *López Díaz* [127], además de destacar los datos de carácter personal de tipo general y hace énfasis en los llamados *sensibles*, asignándole una triple tipología a éstos: a) Datos relativos a la ideología, religión y creencias; b) Datos relativos al origen racial, la salud y la vida sexual de los interesados; c) Los datos referentes a la comisión de infracciones penales o administrativas. Además *Orti Vallejo* [128] , al plantear la anterior tipología de datos sensibles, destaca que los datos relativos a la vida familiar, relaciones personales y patrimoniales entre cónyuges (no las sexuales), relaciones con los hijos, pensiones o costumbres familiares o personales no han quedado incluidas en estos grupos de datos a pesar de merecer especial protección por parte de la LORTAD, quizá, interpreta el autor citado, que es por la tendencia mayoritaria de las leyes de todos los países que afirman que los datos relativos a la vida privada resultan secundarios frente a aquellos que se refieren a las opiniones o ideologías. Sin embargo, conviene reestudiar la posibilidad de que algunos datos íntimos gocen de protección legal, pues tras datos aparentemente inocuos se esconden datos verdaderamente sensibles y viceversa.

Herbert M., establece una tipología de los datos de carácter particular obrantes en bancos automatizados, agrupándolos en muy sensibles, sensibles y neutros, y para cada uno un sistema de garantías diferenciado. La jurisprudencia alemana ha rechazado la diferenciación entre los distintos datos, y apoyándose en la *sensibilidad, no por relación al dato mismo, sino a la vista*

---

(126) SOUVIRON, José M. *En torno a la jurisdicción del poder informativo del Estado y del control de datos por la administración*. En Revista Vasca de Administración Pública. R.V.A.P. No.40, Bilbao, 1994 pág.152-154.

(127) LOPEZ DIAZ, Elvira. *EL Derecho al honor y el derecho a la intimidad*. Ed. Dykinson, Madrid, 1996, pág.243.

(128) ORTI VALLEJO, A. *Derecho a la intimidad e informática*. Ed. Comares, Granada, 1994, págs. 79 y ss.

del contexto y de las finalidades perseguidas[129]

La A*teoría del mosaico*@ de *Simitis,* plantea que datos *ab initio* irrelevantes o Aanodinos@ pueden esconder datos Asensibles@, con el simple cambio de la finalidad que dichos datos perseguía y dado su multi funcionalidad como tales, la interconexión de los ficheros y la libre utilización de los mismos. Datos *sensibles,* se reputaban los relativos a la salud, la vida sexual o las convicciones políticas y, en tal virtud, los sistemas de protección eran máximos, contrapuesto a los datos *libres* que escondían una inocuidad en el espacio proteccionista. Por ello, el autor citado, era partidario que el legislador al regular los sistemas de tratamientos de datos, tome en cuenta la finalidad y el contexto de los mismos, *hasta el punto de conseguir que el éxito de la protección de los datos dependerá, no de una calificación abstracta de los mismos, sino mediante una reglamentación flexible, adaptada a las condiciones particulares de los diferentes tratamientos* [130].

Como antes se observó, en la Ley de Protección de la Intimidad del Canadá, (LPDPC), *Act Privacy* 1983, se incluyen los denominados Adatos sensibles@ dentro de un extenso listado en el art.3, en trece literales, como datos personales o informaciones de carácter personal, sin calificarlos de tal o de diferenciar el grado de protección que a éstos debe darse. En consecuencia, la sensibilidad de los datos personales o su limitado o prohibido descubrimiento, se determina por la condición de ser datos a los que les falta el consentimiento del titular, se hallan bajo el control del Estado y constituyen una causal de excepción (numerus clausus) según el art. 8.2. LPDPC[131].

5.2.3.3. Protección penal de los datos *sensibles,* en el art.197 del C.P.

Sí en el ambiente extrapenal (civil y administrativo principalmente), amplia y fructíferamente han teorizado; entre otros temas, la determinación de los grados de protec-

---

(129). CASTELLS ARTECHE, José M. *La limitación informática*. En: Estudios sobre la Constitución Española. Homenaje al profesor Eduardo García de Enterria. Ed. Civitas, Tomo II, Madrid, Tomo II, 1991.pág. 924
(130). Ibídem..pág. 924
(131) Véase, Artículo 8 de la Ley de protección a la intimidad Canadiense. Nota de pié de página 125.

ción, la clasificación de los datos denominados Asensibles@ y la naturaleza misma de estos datos, a través de la *teoría del mosaico de Simitis,* la cual resulta todavía aún discutible, como hemos visto, en el órbita penal que todavía no ha conformado su propia teoría sobre la sensibilidad de los datos y el grado de protección punitiva gradado que debe suministrarles, a la vista de la clasificación que la propia Constitución (art.16.2), la LORTAD (art.7) y la propia doctrina ibérica han realizado, resulta cuando menos, imprecisa la protección deparada a los denominados datos *sensibles*, por las siguientes razones:

a) Los legisladores del C.P.Esp. de 1995, por A*nítido fundamento y legitimidad político-criminal*@ [**132**], se limitaron a aplicar la técnica de los tipos agravados y ultragravados, cuando un delito contra la intimidad se realice con medios informáticos y/o telemáticos y recaiga sobre datos de carácter particular que revelen la *ideología, religión, creencias, salud, origen racial o vida sexual* (art.197.5 y 6 *in fine*), sin distinción alguna de los datos y el grado de protección deparada por la Constitución y el ordenamiento jurídico.

b) La enunciación *numerus clausus* de los datos considerados *sensibles*, por el C.P.Esp., resulta imprecisa, pues no son todos los que están, ni están todos los que son, como suele decirse. En efecto, como vimos el Convenio Europeo, al prohibir inicialmente el tratamiento automatizado de los datos de carácter personal relacionados con el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, la salud o la vida sexual, así como los datos de carácter personal referente a condenas penales (art.6), establece paralelamente una relación de los datos que considera sensibles, y por tanto, con mayor incidencia en protección legal asignada. Igual cosa sucede con la Directiva 95/46/CE, art. 8. Una simple comparación gramatical del listado de los datos considerados sensibles por el C.P.Esp. (Art.197.5), de una parte; y los estimados tales por las normas comunitarias, de otra parte, es indicativo de que el listado *numerus clausus* del C.P.Esp., peca por defecto. Algunas de las implicaciones por este proceder son las de quedar por fuera de la protección penal datos de carácter personal que las normas consideran sensibles y

---

(132) MORALES PRATS. *Comentarios...* Ob.cit., pág.320

que los doctrinantes las han ratificado.

c) Bien es cierto que al C.P.Esp., no le corresponde resolver el problema surgido por la rebaja en el mínimo de garantías previstas en el Convenio de Europa de 1981 (y diríamos nosotros del mínimo también establecido en la Directiva 95/46/CE), con relación a la LORTAD, tolerante y laxa [133], al permitir lo que inicialmente está prohibido, es decir, el tratamiento informatizado de datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual. Aspecto que incluso es objeto de recurso de inconstitucionalidad ante el Tribunal Constitucional. No es menos cierto, que el legislador de 1995, hizo caso omiso a esa expectativa de inconstitucionalidad sobrevenida y conocida a la fecha de expedición del C.P.Esp., al enlistar algunos de los datos considerados sensibles, los cuales al prohibirse su tratamiento informatizado por disposición legal e incluso constitucional (art.16.2.CE), cuando menos resulta sorprendente, pues su uso legítimo estaría proscrito civilmente previamente antes que recurrir al ámbito penal como *ultima ratio*.

A pesar de ello, parece existir solución al problema desde el punto vista penal dirigida al ámbito extrapenal, como lo denota el profesor MORALES. En efecto, aconseja que se pudiera tratar automáticamente datos sobre el origen racial o vida sexual de las personas, si previamente estos han sido sometidos al procedimiento de disociación, es decir, que el tratamiento de la información personal, previo procedimiento, no asocie a una persona determinada o determinable (art.3, f),), o se *anule la posibilidad de identificar o determinar al titular de los datos*. De esta forma sólo podría tratarse automáticamente datos personales sin identificar a la persona y con fines estadísticos y sociológicos [134].

d) No parece acertada la política legislativa adoptada en el numeral 6, del art. 197 del C.P. Esp., por la cual, se ultragravó con fines de ultraprotección penal, la comisión de un delito contra la intimidad realizado con medios informáticos y/o telemáticos cuando *afectan a datos de los*

---

(133) Ibídem., pág. 321.
(134) Ibídem, pág. 321.

mencionados en el apartado 5, es decir, a los denominados Asensibles@ sólo enlistados: A*ideología, religión, creencias, salud, origen racial o vida sexual*@. Y no nos parece, por el exceso de punibilidad aplicado a la ultragravación, con penas que habiendo sido aumentadas por la agravación del tipo previsto en el apartado 5 del art. 197, con penas impuestas al tipo básico (uno a cuatro años y multa de doce a veinticuatro meses) y aumentadas en su mitad superior, para luego con esta ultragravación, imponérsele además la Apena de prisión de cuatro a siete años@, según el art. 197.6 *in fine*, lo cual a la vista del principio de culpabilidad, como antes se dijo, resulta quebrantado por exceso de punibilidad, máxime si tenemos en cuenta la clase del tipo penal, sus implicaciones sociales y culturales; y sobre todo, la incertidumbre que pone de en evidencia la llamada teoría del mosaico sobre los datos inicuos o irrelevantes considerados sensibles o viceversa, como nosotros estimamos.

5.2.4. El Secreto como visión de la intimidad personal. El ASecreto Informático@.

El Capítulo I, del Título.X,del C.P. Esp.ADel Descubrimiento y Revelación de Secretos@, en el contexto de los tipos penales básicos y agravados, esta cargado de un cierto ambiente provocador a la diferenciación entre la intimidad y el secreto, y de éste último, entre las subclases de secreto general, especiales y el llamado A*sigilium professionalis*@. Sin embargo, tal provocación hoy podría mantenerse sobre las subclases doctrinales del secreto [135], más no, entre el derecho fundamental a la intimidad y el término jurídico, no autónomo, *secreto*. Razones legislativas, doctrinales y jurisprudenciales, llevan a concluir estas premisas. Por lo primero, el legislador anterior al C.P.Esp., siguiendo los pasos de sus antecesores que habían hecho expresa mención al término, *secreto* (art.497 y 497 bis, 498, y 499 ACP.Esp.) y la *intimidad* (art.497bis) como conceptos sujetos a diferenciación, cuando uno y otro términos se hallaban bajo el bien jurídico

---

(135) Al definir el secreto como relación de conocimiento reservado a cierto número de personas y oculto a otras, quedan excluidos los llamados *secretos absolutos*, es decir los que nadie conoce o puede explicar. En tal definición caben, sin embargo, tanto lo que podríamos llamar secretos voluntarios como los fortuitos. *Secreto voluntario* es el conocimiento reservado que permanece oculto a otros por el impedimento consciente del poseedor del conocimiento. En el *Secreto fortuito*, por el contrario, el carácter secreto es independiente de todo actuar consciente de sus poseedores@. Cfr. BAJO FERNANDEZ, Miguel. *Manual de Derecho Penal (Parte Especial). Delitos contra la libertad y seguridad, libertad sexual, honor y estado civil*. 2da, ed., Madrid, 1991, pág. 151

de los delitos contra la libertad y Seguridad de las personas. En aquélla oportunidad, la conceptualización y diferenciación era posible pues se hallaban bajo el cobijo de un bien jurídico distinto de los dos términos referenciados (intimidad y secreto). Hoy en vigencia del C.P.Esp., de 1995, y aunque el legislador persiste en la redacción inclusiva de los términos: Intimidad y secreto, estimamos de importancia capital, recordar que la intimidad, no sólo es un derecho subjetivo de las personas (o de la personalidad, según la teoría civilista), sino un derecho fundamental, ahora erigido como bien jurídico constitucional (art.18 CE y arts.197 a 202 C.P.Esp.)[136]. En consecuencia, la intimidad es un derecho fundamental, y como tal, de la esencia y *conditio iuris* de la protección penal, y también, es un bien jurídico constitucional tutelado y desarrollado en la norma penal, a través de los diferentes tipos punitivos; en tanto, el término secreto que no es un derecho considerado *per se*, ni siquiera un término jurídico unívoco, constituye un recurso gramatical que explica o ejemplifica uno de los aspectos o visiones de la intimidad de las personas, cara a darle contenido a los tipos penales, y nada más.

Doctrinalmente, el profesor *Morales Prats* [137], alude al *elemento subjetivo del injusto*, previsto en el art. 197.1 del C.P.Esp., entendiendo como tal, la intención de vulnerar los secretos o la intimidad de otro. Explica que los *secretos* no constituyen un bien jurídico autónomo o alternativo de la intimidad, y que por tanto, debería haberse optado por la supresión de dicho término, pues el secreto es un concepto jurídico instrumental, en sí mismo vacío de contenido, que puede ser referido a múltiples objetos de tutela y no necesariamente a la intimidad.

Serrano Gómez [138], luego de definir el secreto como *el hecho que sólo conoce una persona, o un círculo reducido de ellas, respecto al cual el afectado no desea, de acuerdo con sus intereses, que sea conocido por terceros*, y establecer inequívocamente que la intimidad es el bien jurídico tutelado en el Cap.X, del C.P.Esp., clasifica los delitos contra la intimidad tomando

---

(136) Véase, apartado 5.1.3.1., sobre el tema
(137) MORALES PRATS, F. *La protección penal* a...ob.cit.,pág. 162
(138) Cfr. SERRANO GOMEZ, Alfonso. Delitos contra la intimidad... Ob. cit., págs.227

como epicentro el concepto de secreto. De esta forma reconoce el carácter de recurso gramatical o instrumental del término frente a la intimidad; pero a la vez, potencia en todos y cada uno de los tipos penales básicos y agravados cuando al *nomen iuris:* secreto, le adiciona adjetivos calificativos que cualifican la figura penal, tales como: documental, telecomunicaciones, profesional, etc.. En efecto, se refiere a los *secretos documentales* (art.197.1), *secreto* de las telecomunicaciones (art. 197.1,parte final), Descubrimiento y revelación de *secretos* por personas encargadas o responsables de su custodia material (art. 197.4.), Descubrimiento y revelación de *secretos* especiales y de menores o incapaces (art. 197.5), Descubrimiento y revelación de *secretos* con fines lucrativos (art.197.6), Descubrimiento y revelación de *secretos* por autoridad o funcionario público (art.198), Descubrimiento de *secretos* por razón de oficio o relaciones laborales (art.199.1), *El Secreto Profesional* (art.199.2) y el Descubrimiento y revelación de *secretos* de personas jurídicas (art. 200).

Más aún, se ha teorizado, sobre el delito denominado A*del Secreto Informático@*[139], *o de violación del secreto automatizado* (art. 197.2) [140], sobre el cual se dice que contiene dos modalidades alternativas y, curiosamente, se trata en primer lugar la que perjudica a un tercero y no al titular del dato o datos automáticamente almacenado, y en cuanto a los Adatos reservados de carácter personal y familiar@ que menciona la norma penal, entiende que son tales, *Aporque el sujeto o no quiere que los conozca nadie o sólo determinadas personas --su médico, su banco,...--* o *la reserva está compartida con una entidad pública por mandamiento legal@.* En tal virtud, considera que a la luz de la interpretación de la norma extrapenal (LORTAD), datos reservados son los contenidos en el art. 2.2.,b), es decir, los referidos a *los ficheros mantenidos por personas físicas con fines exclusivamente personales.* Sin embargo, como también lo reconoce el autor citado una cosa es que estos datos personales y todos los exceptuados en la LORTAD (art. 2.2.), sirvan para explicar la no aplicabilidad de la normativa contenida en la LO 5/1992, y otra muy diferente, que sólo la excepción del art. 2.2, b), sea la interpretación que requerida por el art. 197.2 del C.P.Esp. de 1995.

---

(139) Vid. MUÑOZ CONDE, Francisco. *Derecho Penal*...Ob.cit. pág.221 y ss.
(140) QUERALT JIMENEZ, J.J. *Derecho Penal*...Ob.cit., pág. 198-199.

En efecto, consideramos que el término A*reservado*@, utilizado por la norma (art.197.2), con cierto halo y énfasis del concepto secreto y para calificar a los datos automatizados personales, a la vista de la informática jurídica y las fases del procedimiento o tratamiento automatizado de los datos es equívoco y prescindible sin afectar a la estructura gramatical y jurídica de la norma. Con la mención de ser datos personales automatizados, se explica que éstos son reservados. El término, *reservado*, carece de sentido [141], pues todos los datos personales una vez introducidos en el banco de datos adquieren una sensibilidad (salvo los datos que obren en ficheros accesibles al público, art. 2.2. LORTAD) y protección por parte de la LORTAD. No existen datos automatizados reservados y no reservados, y en consecuencia, todos los datos de carácter personal y familiar automatizados son objeto de protección penal (art.197.2). Actualmente la legislación penal permite clasificar a los datos personales automatizados registrados en generales (art.197.2) y sensibles (art.197.5 y 6), de carácter personal y familiar, sin más calificativo alguno y protegidos y ultraprotegidos por el C.P.Esp cuando el bien jurídico tutelado sea la intimidad [142], sean públicos o privados [143].

Un aspecto capital es *el deber de sigilo por parte de los profesionales de la informática o de los responsables de los bancos de datos (*o Apersonas encargadas o responsables de los ficheros, según el art. 197.4) y su posible violación [144] . Deberes jurídicos ---art. 10 LORTAD-- (y no sólo ético-deontológicos) a los que están obligados por su condición, *status* y labores diarias en un procedimiento de tratamiento automatizado de datos cuando acceden lícitamente a los mismos. Este sigilo, confidencialidad o discreción, es similar a la observada por cualquier otra profesión u oficio. Deber al secreto que según la LORTAD, no sólo se extiende al responsable del fichero automatizado, sino a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal y familiar (aunque omite estos últimos se entiende referido también a éstos). Tanto el secreto, como el deber de guardarlos, son deberes jurídicos que subsistirán aún después de finalizadas sus relaciones con el titular del fichero automatizado o, en su caso con el responsable

---

(141) *Vid. MORALES PRATS* Ibídem., pág. 171
(142) Véase, apartado 5.1.3.3, sobre el tema..
(143) Sin embargo, sí los secretos afectan a la defensa nacional, la revelación es por un funcionario público (caso diferente del art. 198), o la revelación es por abogados y procuradores, se aplicarán los arts. 598 y ss.,413 y 466 C.P., respectivamente. Vid. MUÑOZ CONDE, F. Ob.cit.,pág. 219.
(144) Vid. *MORALES PRATS*, Ibídem. 190

del mismo.

La violación al *secreto profesional*, mediante actos de revelación, difusión o cesión informática o telemática, por los profesionales de la informática, responsables del fichero *y quienes intervengan en cualquier fase del tratamiento de los datos* (según la LORTAD y que caben en la denominación de *personas encargadas*, del art.197.4), según los numerales 1, 2, y 3 del art. 197 C.P.Esp., siguen las mismos planteamientos que hemos realizado en los apartes 5.1.1 y siguientes, sobre los tipos penales básicos , agravados y atenuados (art. 197.3 *in fine*).

Si bien la política criminal del legislador penal de 1995, pudiera tener fundamento especializador, al instituir en el art.197.4 un tipo penal agravado por la condición de los profesionales que laboran en la informática o por ser responsables de los bancos de datos y por su conductas en las fases del tratamiento automatizado o no, no creemos conveniente que se haya procedido a diferenciar a tales profesionales con otro cualquiera también profesional, aunque con diferente oficio y posiblemente relación laboral. Esto plantea una colisión interpretativa del art. 197.4 y 199 del C.P.Esp. La distinción entre unos y otros, es innecesaria, pues como se dijo el deber de secreto o confidencialidad *necesaria* [145] ,es igual para cualquier profesional. Otra cosa es que la LORTAD, haga expresa mención a los responsables de los ficheros y a quienes intervengan en cualquier fase del tratamiento de datos personales, pero para efectos de la aplicación de la misma ley (L.O. 5/1992), pero no para que se les distinga por la ley penal para agravar un tipo penal, o lo que es peor, para tipificar doblemente una misma conducta, en dos normas distintas como sucede actualmente en el C.P.Esp.

Hoy, existe una abundante e incontrovertible jurisprudencia del Tribunal Constitucional y Tribunal Supremo Españoles, sobre la interpretación del *derecho al secreto de las comunicaciones* (art. 18.3 CE), o el *Aderecho fundamental al secreto de las comunicaciones@* (STS, Sent. Abril 2 de 1996. FJ. 6 M.P.: Montero Fernández-Cid), o como inicialmente se denominó: A*la libertad de las comunicaciones, implícitamente y, de modo expreso, su secreto*@ (STC 114/1984, de 29 de

---

(145) AEl personal informático como los responsables de los ficheros deben ser considerados ´confidentes necesarios´@. Un interesante planteamiento al respecto, en MORALES PRATS, Ob. cit.pág.192-193.

noviembre) y el derecho fundamental a la intimidad. El Secreto es el Aconocimiento de ciertos datos sobre un concreto objeto por un número reducido de personas y que, por diversas razones, no es conveniente que se amplíe dicho círculo, siendo relevante la voluntad del titular al respecto@ (STS Mayo 21 de 1993), y también puede decirse que el concepto

> **secreto+, que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales. La muy reciente Sentencia del Tribunal Europeo de Derechos del Hombre de 2 Ago. 1984 -caso Malone- reconoce expresamente la posibilidad de que el artículo 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que, como el llamado en comptage, permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma (Por ello) Sea cual sea el ámbito objetivo del concepto de "comunicación", la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma. La presencia de un elemento ajeno a aquellos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado* **[146]** .

Hoy en día, como sabemos, ese *ilícito constitucional,* a que hace referencia la sentencia del Tribunal, en nuestro criterio, tiene plena regulación legislativa en el C.P.Esp., en el art. 197.1, *in fine* como antes se analizó **[147]**.

Igualmente por vía jurisprudencial se llega a la misma conclusión doctrinal, respecto de la subsunción del derecho al secreto en la intimidad. En efecto, A*El derecho al secreto de las comunicaciones telefónicas tiene el mismo fundamento jurídico que el derecho al secreto de la correspondencia, ´ la protección de la vida privada de las personas´ siendo así considerado como una manifestación más del derecho a la intimidad@,* citando la jurisprudencia del Tribunal Europeo de Derechos Humanos (Sent. de 6 de Septiembre de 1978. C.D.41. **[148]**

Ahora bien, los titulares de ese derecho al secreto de las comunicaciones previsto en el art. 18.3 CE, en particular de las postales, telegráfica y telefónicas, *salvo resolución judicial,*

son:_____**(146)** Cfr. Sent. Noviembre 29 de 1984. F.J. 7. P.M: Díez Picazo

(147) Véase, aparte 5.1.3.2.2., sobre el tema.**(148)** Citada por, LOPEZ DIAZ, Elvira. *Derecho al honor* ... Ob. cit., pág. 224.

las personas físicas y las jurídicas tanto nacionales como extranjeras, mayores y menores de edad, porque el secreto de las comunicaciones presupone la libertad, y su restricción se produce en un sentido de control y observación y no propiamente de impedimento a las comunicaciones y se extiende tanto al conocimiento del contenido de las mismas, como a la identidad de los interlocutores -S.TC. 114/1984, de 29 de noviembre y S. del T.E.D.H. de 2 de agosto de 1984, caso Malone-. [149]

5.2.5. Medios comisivos Ainformáticos, electrónicos o telemáticos@: Sus impactos.

El C.P.Esp., de 1995, pero particularmente el Título X, Capítulo I, de los delitos contra la intimidad, contiene un amplio espectro de términos técnicos de uso corriente en las tecnologías de la información y comunicación (TIC), como en la informática jurídica, pero quizá no tan usual ni de fácil asimilación en el derecho penal, aunque, valga la oportunidad, esta rama del derecho es la que por esencia y condición sine qua nom de *ultima ratio,* tiene que incorporar todo nuevo fenómeno científico, tecnológico, social, político, cultural, etc, que altere, modifique, anule o extinga libertades y derechos constitucionales, normativos o intereses legítimos de las personas.

La inclusión de terminología técnica en la redacción de las normas jurídicas, y en particular, las de naturaleza penal, siendo producto indefectible del desarrollo tecnológico actual e irreversible, por cierto, ha ocasionado algún temor interpretativo a la hora de aplicarlas al caso concreto, ya que el operador jurídico (legislador, Juez, abogado, procurador, etc) debe hacer uso de sus conocimientos generales, especiales y, sobre todo tecnológicos del fenómeno TIC y la informática, a riesgo de que se produzca una *inseguridad jurídica*, devenida por la *forma realmente complicada, con algún artículo interminable y de difícil concreción* como sucede con el actual art. 197 CP.Esp. Como consecuencia de esa inseguridad jurídica, se podría dar una tendencia a archivar los procedimientos o absolver [150] a las personas involucradas en una investigación y juicio penal que tenga como fundamento jurídico la mencionada norma punitiva.

---

(149) Sent. Abril 2 de 1996. FJ. 6. M.P. Montero Fernández-Cid

(150) ADurante el año de 1994 de las 2.563.379 Diligencias previas incoadas por presuntos delitos, sólo 124 lo fueron por descubrimiento y revelación de secretos. *Memoria FGE, 1995, Estado B2.* De estos procedimientos iniciados sin duda que las condenas serán mínimas. Según las últimas estadísticas judiciales publicadas, en el año de 1993.. no hubo ninguna por descubrimiento y revelación de secretos. *Estadísticas judiciales de España 1994,* Madrid, 1996", citada por SERRANO G.A. Ob.cit.,pág. 226

No olvidemos en el fenómeno TIC y la informática, en el Código penal español se hizo efectivo, a través de las llamadas Aescuchas telefónicas@, las grabaciones sonoras, etc., que motivaron la creación de dos preceptos (arts. 192bis y 497 bis, Ley Orgánica 7/1984, de 15 de Octubre) en el anterior C.P., destinados tipificar expresamente la interceptación de comunicación telefónica y utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido. La Ley Orgánica 18/1994, de 23 de diciembre, amplio los tipos a la captación de la imagen, tipificando expresamente la publicación de la información por quien teniendo conocimiento de su origen ilícito, no había tomado parte en su descubrimiento y aumentando sensiblemente las penas [151]. La normas extrapenales del fenómeno TIC y la informática, se halla regulado en la Ley 31 de 1987, de diciembre 18; L.O 5/1992, de 29 de Octubre, de Tratamiento automatizado de los datos de carácter particular, R.D. 1332/1994, reglamentario de la LORTAD, particularmente sobre *el habeas data*. Ley 30/1996, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP) y R.D. 16/2/96, núm. 263/1996, que regula la utilización de técnicas electrónicas, informáticas y telemática por la Administración del Estado; entre muchísimas otras, que surgieron a partir de la LORTAD, (inspirada en normas europeas sobre el tratamiento automatizado de datos personales anteriores y sobre todo, en el Convenio Europeo de 1981 [152]) y en la Directivas 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 [153].

Hoy, se hallan recogidos los anteriores tipos penales y otros que se adicionaron

---

(151) MUÑOZ CONDE, F. Ob. cit., pág. 220

(152) Véase, parte primera y tercera de este trabajo

(153) Existe actualmente una propuesta de Directiva del Parlamento Europeo y del Consejo, 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. ALa propuesta de Directiva, pretende garantizar la libre circulación de los datos y de los servicios y equipos de telecomunicaciones en la Comunidad mediante la armonización del nivel de protección del tratamiento de los datos personales en el sector de las telecomunicaciones y de los legítimos intereses de los abonados a los servicios públicos de telecomunicación que sean personas jurídicas . La Directiva especificará, para el sector de las telecomunicaciones, las normas generales establecidas por la Directiva general sobre el tratamiento de datos personales y potenciará la protección de la intimidad de las personas y de los legítimos intereses de los abonados a los servicios de telecomunicación que sean personas jurídicas@. En: Comisión de las Comunidades Europeas. Bruselas. 05.03.1997. Abril 11 de 1997, págs. 1-11.

en el Título X, *Delitos contra la Intimidad...*, Cap. I, *Descubrimiento y Revelación de Secretos* del art. 197 del C.P. Esp., como hemos visto [154]. Sin embargo, hoy más que nunca, se requiere especificar qué se entiende por medio informático, cuáles se consideran como tales y cómo se emplean en la realización, ejecución o consumación de las conductas delictivas del tipo penal básico o agravadas previstas en el actual C.P.Esp., de 1995; máxime cuando, el operador jurídico se encuentra con términos utilizados por las normas jurídicas, tales como: *A los mensajes de correo electrónico@* (a mero título de ejemplo, pues como vimos antes no es el único medio de comunicación electrónica, hoy en día, aunque sí es el más difundido. Entre otros, están: Foros de debate *--Anewgroups@--*, las conferencias en tiempo real *Achat rooms@* , servicios de lista de correo electrónico *--Amail exploders o list servs@--, la red de redes de hipertexto, imagen y sonido --AWWW@--,* etc)*; interceptación de Atelecomunicaciones@ utilizando Aartificios de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación@; y, los Aficheros o soportes informáticos, electrónicos o telemáticos@*

La urgencia en determinar estos aparentes tópicos, a pesar de que a un sector de la doctrina penal [155], no parece interesarle, es denotar cómo éstos medios informáticos transvasan los límites tradicionalmente conocidos y de todo orden, pues como veremos, las conductas delictivas que hoy observamos , con el nacimiento del fenómeno TIC en matrimonio con los medios informáticos, ya no utilizan una arma física, sino una especie de arma físico-lógica, surgida de la conexión idónea, entre sí de ordenadores o computadores, vía telefónica a través de un modem, un operador de telecomunicaciones, y un programa (software) o Anavegador de comunicaciones @ para cometer atentados contra los derechos fundamentales, patrimoniales o no patrimoniales. *Por ello, hoy, el*
delito de finales del siglo XX y principios del siglo XXI, se caracteriza por la notable,

---

(154) Véase, punto 5.5.2., Parte IV, de éste trabajo.

(155) Nos encontramos con un listado de soportes físicos o lógicos de secretos o de la intimidad idóneos para albergarlos, listado que se cierra con una cláusula general, lo cual no es técnico-legislativamente correcto, pero es una tradición inveterada de la que el C.P.95 no ha sabido desprenderse. La intimidad queda plasmada en un objeto capaz de contenerla (papel, carta, correo electrónico, diskette, tarjeta magnética, cinta de audio o video..). Sea cual sea el soporte conteniendo esa parcela de intimidad, el sujeto lo haya creado o no, debe realizar una determinada acción, a saber, apoderarse del soporte en cuestión. *El medio que empleó para ello, siempre y cuando no resulte constitutivo de otro delito... resulta irrelevante.*Vid. QUERALT JIMENEZ, JJ. Ob.cit.pág.194.

penetrante y porosa sutileza, muchas veces anónima, con que se utilizan los medios físico-lógicos (de hardware y de software) en la comisión de una conducta ilícita

Igualmente, porque el uso, la utilización de los medios informáticos como mecanismos potentes de comunicación y de transferencia de datos o informaciones no tienen fronteras geográficas. Los controles jurídicos empleados por los Estados, aún son muy incipientes a nivel global como lo es el fenómeno TIC y la informática y no simplemente de aplicación sectorial bien estructuradas y desarrolladas para aspectos generales, pero insuficientes y no específicas para éstos medios y fenómenos tecnológicos, tal y como sucede con las normas de corte comunitario (Estados de la Comunidad Europea, UE ; o, incluso los países de la Common Wealth, los del Pacto Andino, los EE.UU, entre muchos otros). Los medios son accesibles a cualquier persona privada o pública, sin parámetros de diferenciación alguno y lo más paradójico, utilizando aparatos, equipos, instrumentos informáticos y sistemas electrónicos conocidos como de A*tecnología punta@*, (fenómeno TIC y la informática). El uso de éstos medios, por regla general, es gratuito en instituciones públicas e incluso privadas (v.gr. Entidades Gubernamentales u organismos del Estado, Centros de educación primaria, básica secundaria, universitaria y postuniversitaria, Centros de Investigación, de Salud, Bibliotecas, etc). La adquisición e interconexión es fácil, de calidad y relativamente barata para todo usuario (que no requiere sino tener un equipo informático y de comunicaciones apto, propio o generalmente facilitado por entidades públicas o privadas). Así mismo, y en similares condiciones de factibilidad sin aparentes obstáculos jurídicos, éticos, culturales y económicos, para quien utiliza, accede, ingresa, difunde información o datos de todo tipo, a través de los medios informáticos.

Este paraíso mundial de facilidades en la utilización de medios informáticos, quizá halle justificación en su mismos orígenes y la amplia gama de prestación actual del servicio y del fenómeno TIC, unido a la masificación de los equipos, aparatos y programas computacionales y; por supuesto, a los operadores de la comunicación (públicos, privados o mixtos, actualmente existentes. v.gr.Telefónica y Retevisión, en España), proveedores de acceso (por regla, privados) y proveedores de la información o datos de toda índole (particulares y públicos). Igualmente, se explica, entre otras razones, por la globalización del

fenómeno TIC (Simil literario de laAAldea Global@), la publicidad rápida y eficaz, competencia de mercados, el acceso, utilización y difusión de datos por vías más penetrantes, certeras, porosas, sin peajes ni cortapisas más que los autolímites de los propios usuarios, tales como, el autocontrol y los códigos de conducta [156]; la normativa general, estatal y comunitaria de protección a los derechos humanos y el control y sanción por los abusos y excesos , como sucede en Francia, por ejemplo, en el *recorrido* de las autopistas de la información, a través de *Internet.*

Uno de los paraísos en donde es posible, hoy por hoy, la utilización de los medios informáticos es en la Red de redes de información más grande del mundo, conocida como *Internet* [157], en donde se potencian estos medios informáticos con los cuales cuenta el ser humano para transmitir, emitir o recibir datos de cualquier índole, en las condiciones especialísimas y con los equipos y sistemas informáticos, antes descritos. En los Estados Unidos, una reciente Sentencia de la Corte, ha puesto en evidencia, esa calidad de paraíso mundial, pues se ha sostenido que *A La*

---

(156) Internet: Red de redes de información entre ordenadores conectados entre sí, a través de una línea telefónica y un MODEM (*MOdulador/DEModulador de señales de comunicación*). El uso y abusos a los derechos fundamentales (principalmente de los derechos de intimidad --*vie privée*--, libertad de expresión y derechos de autor) el conflicto en el ejercicio y de intereses entre los mismos y la protección por parte del Estado, son algunas de las principales preocupaciones de los juristas con la utilización del Internet, tal como lo expone *Isabelle de Lambertiere, Directora de Investigaciones del Centro de Estudios y Cooperación Jurídica Internacional Poitiers, CNRS.París.* Sostiene estos ADeux mécanismes efficaces ont déjà largament fait leur preuve dans la sociétè de l´information. Il s´agit tout d´abord de la solution adoptée en France par France Télécom pour le réseau Télétel qui consiste à contractualiser les engagements, à respecter les recommandations déontologiques. Le non-respect de ces règles par le fournisseur permet à France Télécom d`envisager de résilier ou de supendre le contrat. L`autre technique consiste à promouvoir des codes de conduite. C´est ce qui est fait aujourd´hui dans plusieurs pays pour plusieurs catégories professionnelles d`auteurs (producteurs, serveurs, ...)@. DE LAMBERTERIE, I. *ETHIQUE ET REGULATION SUR INTERNET*. Texto completo En: WWW.UMONTREAL. CA/DOC/DOCTRINA.HTL

(157) ***Internet..*** .es el resultado de lo que empezó siendo un programa militar denominado *ARPANET*, diseñado para transmitir información aun en el supuesto en que algunas partes de la red se vieran dañadas como consecuencia de una acción bélica. Aunque posteriormente se abandonaría el programa militar, sirvió de modelo para la creación de nuevas redes para usos civiles que, unidas a su vez entre sí, permitirían conectar con el paso del tiempo a decenas de millones de personas y acceder a una ingente cantidad de información desde cualquier punto del planeta. ***La internet, subrayará enfáticamente el Tribunal, es el único medio, enteramente nuevo, de comunicación mundial.*** La Internet ha experimentado un crecimiento extraordinario. El número de máquinas que almacenan y proporcionan acceso a la red (*host)* ha pasado de 300 en 1981 a 9.400.000 en 1996. Aproximadamente, el 60% de esos ordenadores están localizados en Estados Unidos. Unos cuarenta millones de personas acceden actualmente a Internet, número que podrá ascender en el año 1999 a los doscientos millones. Cualquier individuo puede acceder a Internet a través de múltiples formas: servidores de red; centro de enseñanza y universidades; centro de trabajo; bibliotecas; computer coffe shops, etc. Los servidores más importantes (*on line services*) como ACompuserve@, AAmerican Online@, AThe Microsoft Network A y AProdigy@, ofrecen acceso a sus propias redes así como la conexión a los principales recursos de la red. Estos servicios comerciales cuentan con más de doce millones de suscriptores en 1996. Todo el que tenga acceso a la Internet puede hacer uso de los distintos métodos de comunicación y obtención de información. Entre los principales están: a) Correo Electrónico (*E-Mail*); b) los servicios de lista de correo automático (*mail exploders o* l*istservs*); c) los foros de debate (*newgroups*); d) charlas o conversaciones en tiempo real (*Chat rooms*); y e) La World Wide Web. WWW. Cualquiera de estos medios permite transmitir sonido, fotos e imágenes en movimiento. Sentencia del Tribunal Supremo Norteamericano, de 26 de Junio de 1997. *Communication Deceny Act de 1996* (CDA). Texto completo en: WWW.UNIDUESSELDORF.DE

ausencia de regulación legal y de control administrativo ha producido sin duda una forma de caos, pero como se afirma en la sentencia del Tribunal de Distrito para el Distrito Este de Pensilvania, de 11 de Junio de 1996, la razón del éxito de la Internet radica precisamente el enorme caos que la preside. Su fuerza descansa en este caos@ **[158]**

5.2.5.1. El Medio Informático en la Sociedad de la información: Las Cibercivitas.

)Qué entendemos por medio informático para el ámbito del Código Penal Español?. Es lo primero que nos preguntaríamos dentro de esta cadena de definiciones técnicas, abundantes a partir de 1995, pero necesarias para comprender y asimilar la terminología que traen las normas jurídicas referidas al nuevo fenómeno TIC, la informática y el derecho penal.

Se entiende por Medio, *el mecanismo, la instalación, el equipo o los sistemas de tratamiento de la información que permite, utilizando técnicas electrónicas, informáticas o telemáticas, producir, almacenar o transmitir documentos, datos e informaciones*. (art.3, b), R.D. 263/1996, 16 de Febrero). En esta definición se incorpo- ran *in genere* los medios físicos o materiales, tanto referidos al denominado *Hardware* (el ordenador, propiamente dicho y las unidades periféricas **[159]**), como a los medios lógicos, logiciales o de *software* (programas de ordenador), utilizados en el procedimiento o tratamiento automatizado de todo tipo de información o datos. Así mismo, a todos aquellos aparatos o sistemas electrónicos que no haciendo parte del hardware o el software, sirven a los fines y objetivos informáticas, al complementar o potenciarlos. Tal es caso del conjunto de aparatos y sistemas de telecomu-

---

(158) Cfr. Sentencia del Tribunal Supremo Norteamericano, de 26 de Junio de 1997, por la cual se confirma y declara la inconstitucionalidad de determinados preceptos de la *Communication Deceny Act de 1996* (CDA). Texto completo en: WWW.UNIDUESSELDORF.DE

(159) Unidades periféricas o también llamados en informática Asoportes informáticos@, porque rodean, auxilian y complementan el procedimiento informático iniciado en la Unidad de procesamiento central (CPU) del hardware. Podemos clasificarlos, así: a) unidades periféricas de entrada de información (E/): teclado, el puntero electromanovisual o Amouse@, lectores ópticos (lápices), tableros electrónicos, unidades de rayos infrarojos (eliminan cables), cámaras de vídeo (muy sofisticadas como la de vídeo digital Canon DM-MVI, videocámara que permite captar imágenes en movimiento y pasarlas luego al ordenador, en donde podrán editarse: seleccionar y retocar imágenes individuales, etc.) y todos aquellos que se elaboren en el futuro con este fin, b) unidades periféricas de salida de información (/S): a) Monitor, las impresoras, plotters, scanners, cámara de vídeo, etc. Un estudio más amplio en mi trabajo, *Constitución 1991 y la informática jurídica*... Ob. cit., pág. 128 a 234.

nicaciones unidos a los eléctricos y/o electrónicos que sirven para captar, editar, emitir o transferir imágenes, sonido o texto; o todo a la vez, pues al fin y al cabo todo esto *es información*[160] bien representada analógica o digitalmente. v.gr. las fotografías en el espacio del Internet[161],evidencian la vulnerabilidad de la intimidad, a través de la imagen.

La capacidad de estos medios físicos o lógicos para captar, procesar, editar y entregar información o datos por cauces electrónicos, informáticos o telemáticos, es lo que determina que estos medios se les denomine globalmente, a los efectos de éste trabajo investigativo, *medios informáticos*. Por su parte, la LORTAD, en su exposición de motivos, y en el sentido antes plantado, hace alusión a los medios informáticos cuando explica que APartiendo de que su fina-

---

(160) Sí la información nos proporciona conocimiento, entonces es un concepto referible a los seres humanos, pero puede extenderse también a los ordenadores o, en general, a cualquier sistema con posibilidad de percibirla y en consecuencia de variar su estado. El receptor de la información, con su capacidad de asimilación (bien sea incremento de incremento del conocimiento, o cambio de estado), es, pues, una parte esencial del concepto. Otra lo es el mensaje que aporta la información, compuesto de elementos perceptibles a través de los sentidos (o sensores, en el caso de una máquina) del receptor. Y naturalmente si hay mensaje habrá también un emisor, a veces otra persona pero, en términos más generales, un sistema que, como el receptor; es dinámico. Consideremos ahora el mensaje. Tres son las operaciones que pueden realizarse con él, además de su generación y recepción. La memorización, para conservarla en el tiempo, la transmisión , que lo lleva de un punto a otro del espacio, y la transformación, para eliminar detalles innecesarios, asociar informaciones de diferentes mensajes o disponerlo bajo formas que pongan de manifiesto aspectos relevantes. La copia (memorización múltiple), el cálculo (transformación bajo reglas matemáticas), la presentación (disposición sobre soportes perceptibles por las personas, destinados o no a la conservación), la ordenación y compilación de diferentes informaciones, la difusión a múltiples receptores, etc., son importantes operaciones derivadas de las anteriores. En la composición de un mensaje pueden distinguirse los niveles físico y simbólico. El primero es el medio (Luz, sonido, ondas electromagnéticas, estimulo táctil, registro magnético en cinta o disco, disco compacto, papel y tinta, etc) cuyas variaciones lo conducen y hacen perceptible. Naturalmente, tales variaciones pueden verse alteradas por la interacción con fenómenos indeseables o problemas producidos en las operaciones anteriores. El ruido que provocan, imposible a veces de eliminar, reduce y hasta puede anular la información contenida en el mensaje. El aspecto simbólico lo constituye el significado, en términos de información, que contiene. Las variaciones del medio físico se han producido siguiendo ciertas reglas que son el código para reproducir e interpretar el mensaje. REPRESENTACION DIGITAL DE LA INFORMACION. Los códigos para representar la información pueden ser analógicos y digitales. La forma analógica consiste en recoger y transmitir variaciones continuas en el fenómeno sobre el que versa el mensaje.... Una fotografía y un registro fenogrático constituyen, respectivamente formas analógicas de memorizar una imagen y un sonido. En la representación digital de la información se parte de reducir el universo de caos posibles a un conjunto numerable y de asignar a cada uno de ellos uno o varios símbolos elegidos de entre un repertorio finito.... Cualquier información es susceptible de ser digitalizada. Una imagen, por ejemplo... De igual manera es posible digitalizar una secuencia de imágenes (película)para reconstruir unos hechos. Para digitalizar un sonido se toma un dato del mismo varias decenas de miles de veces por segundo... El pensamiento se ha expresado y conservado siempre en forma digital, a través de los lenguajes... Estos... son códigos que soportan el mensaje y reducido el número de elementos en que se basan (fonemas, letras, palabras, frases, etc), los símbolos que lo digitalizan. Pero además, y por basarse en un conjunto numerable de símbolos y reglas, cualquier código puede traducirse a otro de tipo numérico. De ahí el nombre de digitalización (conversión a dígitos). Y es bien conocido que cualquier número puede expresarse finalmente tan sólo con dos símbolos diferentes (p.e. 0 y 1), a los que también se les denomina *bits. Así pues, toda información, cualquiera que sea su naturaleza, puede convertirse finalmente en una secuencia de bits@ Cfr.* FERNANDEZ B., César. Ob.cit. pág. 50.

(161) Véase, MIKUS, Jean-Philipe. *LES PHOTOGRAPHES ET LE DROIT SUR LE RESEAU INTERNET. (Jpmikus@colby-monet.com).* AInternet un red mundial con todas la ventajas e inconvenientes de la tecnología numérica@. KELMAN, Alistair. *)Que faire des paparazzis (Stalkerazzi)?*(jdo@lac.gulliver.fr). Caso Lady Diana.

lidad (referida a L.O 5/1992) es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos *por medios informáticos*, la Ley se nuclea en torno a los que convencionalmente se denominan ´ficheros de datos´: Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor@. Sin embargo, en el texto normativo, la ley guarda silencio en cuanto a qué se debe entenderse por medios informáticos, muy a pesar de que el ámbito objetivo de la LORTAD, se les vuelve a mencionar como mecanismos, instrumentos o elementos por los cuales se hace efectivo el tratamiento automatizado de los datos personales (art. 1), cuando es lícito o cuando se prohíbe sí estos son fraudulentos, desleales o ilícitos (art.4.7.).

Muy a pesar de que los medios informáticos teóricamente se pueden clasificar en físicos, materiales o de hardware y lógicos, inmateriales o de software, empleen o no la tecnología TIC, todavía rondan un cierto fantasma o temor que no sólo ronda a los juristas sino para los propios tecnólogos TIC, a los estudiosos de la informática y en general, a la sociedad toda. En efecto, la llamada *sociedad informatizada* necesita de medios, aparatos y procedimientos electrónicos, como de sistemas de tratamiento informático del fenómeno TIC, para su diario vivir, producir y desarrollo, y sobre todo, para comunicarse y transferir información o datos de cualquier índole.

Todo lo que toca la tecnología inmediatamente produce todo tipo de debate, pero esencialmente, de carácter ético, económico, político y jurídico. En éste último, --que nos interesa destacar por ahora--, se produce, cuando menos, por la porosa vulnerabilidad y la correspondiente utilización por parte del Estado de mecanismos jurídicos de protección de derechos, libertades o intereses legítimos en el ámbito del derecho privado, público y penal; así como también, por los altos grados de insidiosidad de los medios utilizados para cometer conductas típicamente informáticas que llevan aparejados un innegable *control tecnológico* de las personas, con claras características de permeabilidad y de potenciación (por ser un control certero, sistemático, penetrante e indivisible [162]) y de insospechados efectos, aún no develados en su integridad, ni siquiera por la misma tecnología TIC, en donde muchos de estos efectos todavía se manejan con criterios de ciencia ficción, tal como ocurrió con la identificación y estructuración de ese espectro global de la comunicación, a través de medios

informáticos, sin ubicación geográfica específica , a pesar de tener cobertura en todo el mundo y abierto a cualquier persona que tenga acceso a *Internet*, bautizado por la literatura como de *ciberespacio* [163]. A partir de allí todos los subproductos tecnológicos, sociales e incluso jurídicos catalogados con el prefijo *Aciber@* (v.gr. ciberdelito, ciberpolicía, cibernauta ,etc) y que forma una curiosa, no plenamente analizada, *cibercultura*, que va incursionado en todos los terrenos de la sociedad informatiza actual, y por supuesto en el derecho, como veremos.

Por paralelo, nacen algunas preocupaciones comprensibles sí, pero muchas no justificables, que se traducen luego en verdaderos temores Algunos de éstos devienen del concepto mismo de *medios informáticos y/o de sus efectos.* Veamos algunos:

a) Un cierto temor a la terminología técnica en el derecho extrapenal, se logra paliar recurriendo al simil literario [164] . No en vano se entiende el esfuerzo por explicar la estructura de la red de redes de información y comunicación *internet* (llamada *democrática*, por que se puede acceder y recorrer en todas las direcciones posibles tras una información útil o sutil), la red *Milnet* (conecta a altos mandos militares) y la red *Swift* (que posibilita transacciones electrónicas entre entidades bancarias y bursátiles) y analizar en que medida afecta a los derechos de los ciudadanos la convivencia con las nuevas tecnología, con esa ***nueva cultura***, llamada

(162) Vid. MORALES PRATS, F. Ob. cit., pág. 153

(163) El término *Ciberespacio (ACyberspace@),* fue acuñado primero por el escritor de ciencia ficción, William Gibson, y se aplica al espacio electrónico (la comunidad o nuevo mundo virtual) creado por la comunicación, a través de equipos o aparatos computacionales interconectados entre sí. La adopción extendida de la tecnología de las redes de comunicación, ha producido un nuevo medio, por el cual se transfiere información entre las personas. Las implicaciones legales de tales actividades son ignoradas a menudo por los usuarios y operadores de redes de comunicación, máxime cuando los riesgos (Apitfalls@) son numerosos. Hasta hace muy recientemente, el conocimiento sobre el uso de las redes de información por computadores, era prácticamente restringido para un gran sector de la comunidad e incluso para los versados en las ciencias jurídicas, pues el ´´cyberspace´, sigue considerándose, una región de frontera por la que transitan los pocos aborígenes de la tecnología (Aaboriginal technologists@) y los Acyberpunks@ (gamberros del ciberespacio), quienes pueden tolerar la austeridad de ésta con las salvajes computadores que los une, a través de protocolos incompatibles de comunicaciones, obstáculos, ambigüedades culturales y legales, y en general, por la falta de mapas útiles o metáforas´. Cfr. Nikos Drakos (nikos@cbl.leeds.ac.uk). ALegal Pitfalls in Cyberspace: Defamation on Computer Networks@. Texto completo en: *WWW.UMONTREAL.CA.* En sentido similar, la Sentencia del Tribunal Supremo de los Estados Unidos, 26 de junio de 1996, que considera al Ciberespacio como Ael conjunto (de) todas estas herramientas (se refiere, a los E-Mail, Mail Exploders, Newsgroups, chat rooms, y el WWW) constituyen un medio de comunicación unitario y único..., que no se encuentra ubicado en ningún lugar geográfico, está abierto a cualquiera que tenga acceso a internet, desde todos los puntos cardinales@. Texto completo en: *WWW.UNIDUESSELDORF.DE*

(164) Son continuos y reiteradas las remisiones a la literatura para explicar los avances tecnológicos TIC y la informática v.gr. Alos peligros del denominado ´totalitarismo virtual@ (Michel Foucault), para explicar los efectos de las nuevas formas de control de la persona (en MORALES PRATS, ob. cit., pág. 153).)Quo vadis, internet?. Un estudio que plantea cinco posibles escenarios futuros de la red. *La Vanguardia*. Domingo 18 de Enero de 1998. AEscándalo sexual en la casa blanca catapulta el periodismo electrónico. Clinton@Lewisky.net@. *La Vanguardia*. *D*omingo 1 de Febrero de 1998. AHacia las autopistas de la (in)formación@. Gabriel Ferraté. *LA VANGUARDIA.* Domingo 11 de Enero de 1998. *La inteligencia colectiva*., según el filósofo francés, Pierre lévy, una utopia que puede ocurrir con internet. En: Diario LA VANGUARDIA. Domingo, 8 marzo de 1998

A*Telépolis*@[165] . Telépolis es una ciudad, con calles, plazas y con múltiples direcciones y accesos, con lo la hacen la ciudad más grande del mundo, quizá la única, pues el simil de Aaldea global@ a esta *cibercivitas,* sin fronteras geográficas (que subsuman controles jurídicos o de cualquier otro tipo debidamente regulados con carácter transfronterizo, actualmente inexistentes en alguna parte del mundo, a lo sumo, pudiera pensarse que sí lo están con ámbito sectorial. p.e. La Unión Europea, en materia probatoria penal [166], los países de la Common Wealth, El Pacto Andino, EE.UU, etc) y por su puesto los pobladores, los *cibernautas* (navegadores o usuarios privados y/o públicos de la red), de cualquier edad, pueden interconectarse para intercambiar información de todo tipo, pero principalmente, personal o familiar, cultural, político, laboral, científica, técnica o investigativa. La comunicación de los cibernautas o *internautas* [167] mediante aparatos electrónicos y sistemas informáticos (en la que intervienen: *operadores* --empresa de telecomunicaciones--, *proveedores de conexión, o mejor, proveedores de acceso* [168] --dan paso al uso de la red: Apeaje@ con contraseña: password--, y *el proveedor de contenidos* –pone la infor-

---

(165) Nombre tomado de Echevarría, Javier, por GONZALEZ NAVARRO, Francisco. *Comentarios a la ley de Régimen*... Ob. cit., págs. 823-827

(166) Obviamente que la Comunidad Europea, viene ampliando cada día la órbita de compatibilización normativa de cara a paliar los efectos globales del fenómeno TIC, la Informática y los nuevos equipos y aparatos de telecomunicaciones, sobre todo en el ámbito penal que es donde parece golpear con mayor fuerza y de ahí los ingentes esfuerzos por los Estados Democráticos actuales para minimizar los impactos de las nuevas tecnologías. La UE, mediante la Recomendación (95)13 Adoptada por el Comité de Ministros de 11 de Septiembre de 1995, recomienda a los Estados de la Unión, se tomen las medidas normativas y jurídico-procesales, en relación con los Aproblemas suscitados en las leyes de procedimiento penal cuando se vean involucrada las nuevas tecnologías de la información@, particularmente en materia probatoria: solicitud, decreto, práctica, evaluación, validez y eficacia de la prueba recolectada y aplicada a los procesos penales en su fase de investigación o juzgamiento, en los que se vea involucradas las nuevas tecnologías TIC, los computadores o sistemas informáticos. Se recomienda además, compatibilizar las normas sobre pruebas en el campo penal, la cooperación internacional para la lucha contra el crimen informático y si fuese del caso proceder a la Ainterceptación de las comunicaciones@, previa la autorización judicial o de la ley, a fin de identificar la fuente de las comunicaciones y conductas delictivas. Esta recomendación revoca otras anteriores en sentido parcialmente similar a la presente, tal como la Recomendación (85) 10, sobre cartas rogatorias para la interceptación de telecomunicaciones. Recomendación (87)15, Sobre el uso de datos personales en el Estado policiaco y la Recomendación R(89) 9, Sobre Delitos mediante computadoras. El anexo, precisa una terminología propia de la tecnología TIC y de la que dado cuenta en el texto principal del trabajo, tales como: a) Evidencia electrónica, b) Uso de la Encriptación de información o datos (AEncrytion@). Texto completo en WWW. UMONTREAL.CA.

(167) La terminología generada por el fenómeno TIC y la informática, por el uso o manipulación de medios, aparatos electrónicos y sistemas informáticos, es cada día más abundante, pone de manifiesto la porosidad y saturación que aquéllas conllevan y el replanteamiento lexical y gramatical del propio idioma. Bajo el título sugestivo de *)Es usted un intervívoro?.* Pone en tela de juicio y satiriza las innumerables Apalabrejas@ nacidas por la informática. Vid. *LA VANGUARDIA.* Barcelona, Domingo, 7 de Diciembre de 1997.

(168) Hacemos el énfasis, para entender mejor el procedimiento de tratamiento de la información y la terminología utilizada tanto por el C.P.Esp., como por los iusinformáticos al comentar el fenómeno TIC y la informática. Algunos de los proveedores de acceso a internet en España, son: SIEMENS, ARGO, JET, TELELINE, VALLES SERV, CTV, READYSOFT, LANDER, GRN, IndecNet. Un estudio comparativo del mercado y competencia salvaje al que se hallan expuestos estos proveedores, lo podemos ver en: *Diario La Vanguardia*. Domingo 15 de Feb.del 98.

mación: instituciones públicas y privadas--) potencian los vehículos o canales (como la voz, símbolos, imágenes, expresiones, etc.) que portan un mensaje escrito, visual o audio-visual, de imágenes gráficas o fotos digitalizadas, o imágenes en movimiento, voz real o digitalizada, etc. Los mensajes de correo electrónico, los servicios de lista de correo automático, los foros de debate, las charlas o conversaciones en tiempo real, las páginas WEB (*WWW*) y alta tecnología TIC e informática que se concreta en llamada *multimedia o hipermedia (*que emiten y recepcionan, a la vez, texto, imágenes fijas --fotografía digitalizada-- o en movimiento --escenas de vídeo-- y sonido: humanos, animales, mecánicos o electromecánicos, sectorial o globalmente). Así, la comunicación de datos e informaciones en la *cibercivitas* no sólo es más democrática, sino que es más poder que nunca.

b) El fenómeno calificado de AApocalipsis 2000", AY2K@ o Aefecto 2000" [169], se caracteriza por el desfase de tiempo ocasionado en medios electrónicos y aparatos informáticos, una vez se haya arribado al año 2000. Los ordenadores marcaran en su calendario interno (programados automáticamente, casi todos ellos hasta el año 2050, aproximadamente y lo que es peor ya están en manos de usuarios públicos y privados), como si estuviéramos en el año de 1900 y no en el tiempo real del 2000, con una simple fórmula de dos dígitos que marcan DIA/MES/AÑO (01/01/00): 1 de Enero del 2000. Se dice, que esto ocasionará despropósitos temporales en gestiones públicas y privadas, en actividades bursátiles o económicas, sanitarias, educativas, y sobre todo jurídicas, v.gr. en el ámbito penal, sobre aspectos punibilidad, cumplimiento y ejecución de penas, revisión de prontuarios, etc., salvo si se toman medidas necesarias (políticas, jurídicas, tecnológicas, entre otras) por los Estados y sobre todo, por los tecnólogos TIC y empresas fabricantes de hardware y software informático, para que esto no suceda.

---

(169) El fenómeno consiste en que llegado en el año 2000, los aparatos electrónicos y aplicaciones informáticas, representarán electrónicamente la fecha con un escueto A01/01/00" (1 de Enero del 2000), con sólo dos dígitos para meses, días y año. Este insignificante error es de cien años, pues inmediatamente se volverá al 1 de enero de 1900, según lo indicará el calendario memorizado en los aparatos informáticos, sino no se toman medidas de prevención por parte de los Estados, el sector empresarial y los particulares. Vid. Diario EL MUNDO. Domingo 17 de 1998, Barcelona, (Esp.) pág.11-12.

c) En los sectores extrapenales, la Agencia de protección de datos Española, *es una entidad de derecho público, con personalidad jurídica propia y plena capacidad pública y privada,* (art. 34 LORTAD) que tiene una serie de funciones; entre otras las cuales se destaca la de vigilancia y control (art. 36 LORTAD). Sin tomar en cuenta el debate de inconstitucionalidad que pesa sobre esta institución administrativa *de régimen y estructura sui géneris,* digamos en éste aparte, que el temor que le asalta, según su actual director [170], es la dificultad para controlar la Red de redes o Internet, integrada por ordenadores conectados entre sí desde todos los puntos del mundo, Apero habrá que tratar de limitar para que los derechos fundamentales de las personas no sean contravenidos@. Ciertamente el peligro que asecha a los derechos constitucionales y normativos con el manejo de la red internet, es en todos los ámbitos, por ello, en el derecho norteamericano ha dado origen al llamado *netlaw*, al cual nos referíamos antes, como un producto de las tecnologías TIC e informática en la *cibercivitas* y el esquema de regulación normativa que actualmente tienen sobre la utilización de pistas, redes, medios, aparatos y sistemas informáticos más corrientemente que bibliotecas, librerías, y servicios públicos y privados de todo tipo, sea cual fuera el usuario (público o privado) y el volumen de información o datos (incluso por Apaquetes@,como se suele llamar a los grandes volúmenes de información transferida de un lugar a otros por medios electrónicos).

d) En España [171], la creciente A*Ciberdelincuencia@*[172] comienza a crecer impresio-

---

(170) Vid. AEl Magistrado Juan Manuel Fernández López. Director de la Agencia de Protección de Datos. Sostiene: téngase en cuenta que el avance de las tecnologías tendrá que analizarse para Apoder conjugar los dos intereses: la protección de la intimidad de los ciudadanos y el desarrollo de la tecnología moderna. La agencia, que inscribió en sus registros casi 200.000 ficheros en su primer año de funcionamiento, ha tramitado numerosas denuncias y expedientes sobre las bases de morosos y sobre cesión de ficheros, y ha impuesto sanciones económicas a los violadores de la LORTAD@. Diario *LA VANGUARDIA.* Barcelona, Domingo 29 de 1998, pág. 41.

(171) En España, los delitos más frecuentes son contra la propiedad intelectual (Cuarto país en Europa en denuncias por piratería en 1997). El blanqueo de capitales procedentes de organizaciones mafiosas y propaganda nazi o terrorista es cada vez más frecuente... Los delitos cometidos por la Red no son ni mucho menos significativos en comparación con el uso que de ella se hace. Cfr. Diario *EL MUNDO.* Barcelona, Domingo 1 de Marzo de 1998.

(172) En Marzo de 1994, se conoció el primer caso de difamación por Internet en Australia. David Rinos (sci.anthropology), académico en Australia Occidental, lector regular y colaborador habitual de las páginas WEB, en los Grupos de debate sobre Antropología (AAnthropology news group@), fue demandado por difamación, por Gilbert Hardwick, como resultado de dos mensajes de correo electrónico enviados a un foro de debate (News groups). La Corte Suprema de Australia Occidental, a parir de este caso, reconoció que la información que viaja por el internet A*ya no puede ignorar la ley*@. Se dibuja así al ciberdelincuente. Cfr. Nikos Drakos (nikos@cbl.leeds.ac.uk). **A***Legal Pitfalls in Cyberspace: Defamation on Computer Networks@.* Texto completo en: *WWW.UMONTREAL.CA.*

nantemente como producto de la fácil y Aabusiva@ o Adañina@ (con carácter delictiva) utilización de medios electromagnéticos lógicos y físicos (programas de ordenador y aparatos informáticos y telemáticos), masificados por los bajos costos en el mercado y por el fácil acceso de cualquier persona que disponga de un ordenador, un modem, un teléfono y le sobre ganas de pasearse a su antojo y sin control por las denominadas Aautopistas de información@ (término acuñado por B. Gates), a través de redes de información o de telecomunicación transfronterizas (v.gr. Internet). Los intrusos o fusiladores de datos (Ahackers@[173]) o los rupturadores o destructores de datos (Acrackers@[174]), por regla, general van en busca de información o datos de todo tipo (personal, económica o financiera, política e incluso que interesan o afectan a la defensa y seguridad de los Estados. v.gr. los asedios constantes a los sistemas informáticos del Pentágono realizados por Kevin, el cracker Ade los ochentas@). Por ello, en España se creó en Julio de 1995, A*la Ciberpolicía*@, es decir, la AUnidad de Delitos informáticos de la Policía Nacional@, y en Noviembre de 1996, el AGrupo de Delincuencia Informática de la Guardia Civil@,

---

(173) Kevin Mitnick Shack, es un *cracker,* destructor de datos informáticos y no simplemente un intruso o *hacker* de información o datos. Kevin, se le ha considerado uno de los más famosos hackers de los años ochenta y fue condenado a un año de prisión, convencido el juez de que se trataba de un Aadicto a los computadores@ (*he was a computer addict).* Este A*loco*@de los computadores, ha generado una gran cantidad de artículos y escritos en las páginas WEB de Internet, de conformidad con el asunto en el que se vio involucrado. El más reciente es: AKevin... in honor of the fight to help defend Bianca´s Smut@. Web Articles: a) Mar 20, 1996 "Takedown": A Postmodernist Romance, Jim Thomas, Computer Underground Digest, b) Mar 9, 1996 Hackers on the Web Part II, Discovery Channel Online, c) Feb 1, 1996 Sex, Lies & Computer Tape: On the Trail of Kevin Mitnick in Tsutomu Shimomura's Paean to Himself and Jon Littman's "The Fugitive Game", CRYPT Newsletter, d)Dec 30, 1995 Mitnick's Malice, Shimomura's Chivalry, Scott Rosenberg - SALON, e) Jul 2 Examiner : Hacker agrees to plead guilty, f) Mar 14 GNN: The REAL Story of how Mitnick was apprehended (parody), g) Mar 9 SIMBA : Hacker Inspires Movie, h) Feb 27 Time : Kevin Mitnick's Digital Obsession, i) Feb 27 Time : Cracks in the Net, j) Feb 23 NetWatchers : Most wanted hacker in the world, k) Feb 23 Nando Times : Security is lost in cyberspace, l) Feb 22 Nando Times : Hackers are everywhere, m) Feb 20 Tacoma News Tribune : Cyberspace Dragnet Snared Fugitive Hacker. Un lista completa en WWW.UMONTREAL.EDU.CA.

(174) La piratería informática y el mundo virtual que crean de *crackers* en el mundo ha conformado actualmente una cualificada estadística de los más famosos: a) *Christopher Shanot***.** 1994. Detenido por acceder (Arobar@,según la fuente) inutilizar, destruir y comercializar (sabotaje informático) datos confidenciales de organismos gubernamentales. Integrante del llamado AFrente de Liberación de Internet@. b) *Steve Fleming.* 1994. Escocés. Piratería de datos o informaciones confidenciales de los Servicios secretos y la Familia Real Británica. c) *Kevin Mitchnik*. Pirata que ha ingresado en las redes del pentágono. Accedió a datos empresariales. Detenido por el FBI, en 1995. d) *Antoni Chris Zboralski*. Francés. Detenido en 1995 Acceso a información privilegiada y cargar a la cuenta de AT&T, facturas inexistentes. Realizo sus actos interceptando una llamada telefónica y enterandose del nombre de un agente del FBI en París, Thomas Baker, y e) *Vladimir Levin*. El matemático ruso accedió a redes financieras de Norteamérica e hizo traslados a cuentas de otros países. Detenido en UK, 1995. Vid. *Diario La Vanguardia*. Barcelona, 15/04/ 1998.

para la prevención y la detección de los A*ciberdelitos*@[175] que requieren personal cualificado formados especialmente en informática y redes.

e) Entre otros, la intimidad [176], el correo Abasura@ (*electrones junk*) [177] y la pornografía on line (el *ciberporn* [178]), se catalogan como aspectos importantes, conflictivos en _____

(175) Las actividades de las llamadas AUnidades , destinadas a perseguir al *ciberdelincente* ha sido corta pero intensa@. Dos de las operaciones más importantes realizadas son: a) La denominada ATornado@ a finales de 1996, sobre piratas de software a través de Internet. En febrero de 1997, terminó con arresto de dos personas en Barcelona y otra en Tenerife, acusados de delinquir contra la propiedad intelectual; y, b) La denominada AToco@. Se denuncia por parte de la Universidad Rovira i Virgili (finales de1996), el ingreso no autorizado en la red de su servidor, por parte de intrusos y destructores de datos académicos, bibliotecarios y de seguridad de la Universidad.. A través de los ASniffers@ (programas creados para rastrear claves de acceso: A*Olisqueadores*@) capturaron los passwords de los hackers y crakers hispanos. Cfr. Diario EL MUNDO. Domingo 1 de Marzo de 1998, pág. 15.

(176) AEl derecho a la intimidad, en efecto, plantea problemas nuevos y específicos en el mundo de las redes. Si atendemos a las eventuales lesiones que puede padecer, el peligro reside en el propio servidor de red, aunque se trate de una empresa privada y no de un poder público. En segundo lugar, no ha de olvidarse que los gobiernos nacionales y sus agentes pueden no sólo vigilar la red, sino incluso descodificar mensajes secretos si lo consideran necesario y, a tal efecto, han de respetar ciertas garantías (autorización judicial, v.gr.). Ante el derecho a la intimidad se dan cita toda una suerte de intereses contrapuestos: de un lado, constituye un derecho fundamental básico, señala la frontera entre el Estado y el Individuo; de otro, sin embargo, una protección absoluta ampara y encubre la criminalidad organizada. Es al tiempo el lugar de encuentro de dos concepciones enfrentadas: para unos, la comunidad virtual significa transparencia, se acude a ella para comunicar e informar, no para esconderse en el anonimato. Para otros, por contra, la intimidad y el anonimato constituye elementos fundamentales y de enorme utilidad al servicio de la libre expresión e intercambio de pensamientos e ideas. Por último, la intimidad es esencial para el comercio en la red (secretos o datos reservados de las empresas; estudio y preparación de operaciones económicas a través de la red; datos bancarios; tarjetas de crédito; etc). Y, al contrario, la intimidad supone un límite o un freno a las actividades económicas y empresariales del futuro si se considera que en la era de la información difícil será poder sobrevivir sin una información y una publicidad más personalizada acerca de los clientes@. BARNES V.Javier.La ***internet y el derecho. una nota acerca de la libertad de expresion e informacion en el espacio cibernetico***. En: Revista C.S.J.P., Madrid, 1997, pág.246

(177) AEn la actualidad es evidente que el servicio de la WWW resulta menos permeable a la normativa, puesto que el usuario se limita a elegir por sí mismo los que quiere ver y lo que no. En cambio, la *USUNET* o red de noticias (foro de debates), que fue el servicio más popular de la internet durante mucho tiempo, presenta conflictos de toda clase. Aquí concurren y se intercambian muchos miles de mensajes públicos cada día. Por ello, en esta sede, se hace sentir la necesidad de establecer mecanismos de resolución de conflictos, con mayor claridad que en otros ámbitos. Ello explica que sea también aquí donde haya surgido el cuerpo más denso de costumbres. Algunas de las prácticas y costumbres vigentes son expresión de la eficacia o de un cierto orden en el tráfico; responden a las buenas maneras; o son encarnación de comportamientos éticos. Además, es de destacar la existencia de tribunales de arbitraje; organizaciones de defensa del consumidor; y , desde luego, de todo un aparato sancionador (que va desde la reprobación, pública o privada, a la exclusión del mensaje, si se trata de un foro, hasta por ejemplo, Ael bombardeo@ del buzón de correo --envío masivo de datos inútiles, hasta el colapso@. Citado de A The NetLaw Library@, por BARNES VASQUEZ, Javier. *LA INTERNET...,* pág.246. Ciertamente, no hay más que mirar los buzones de correo electrónico abiertos por cualquier persona (Ausuarios@), previa firma electrónica de contrato de adhesión o aleatorio de servicios de *E-Mail, con el servidor de la comunicación electrónica* (el típico: AI accept@).Servidores internacionales de redes, como Nestcape o Microsoft, por ejemplo, para observar que desde el anuncio de bienvenido al servicio (AWelcome@) y por todo el tiempo que mantenga el *Mail-box*, éste estará infestado de publicidad, correo interno del servidor; y en fin, de correo Abasura@. Este lo seguirá al usuario, como la sombra al cuerpo. Vid. Parte III.

(178) *El ciberporn*, está constituido por el ingreso, acceso, utilización, difusión o publicación y transferencia fuera de sistema de imágenes digitalizadas (o fotografías por ordenador) o en movimiento (video) con sonido, texto o sin ellos, que muestren el cuerpo humano, su genitalidad, el acto sexual normal o anormalmente (v.gr. zoofilia, necrofilia, etc) de personas de cualquier edad o sexo y han sido Acolgados@ o colocados en las páginas del WEB de internet, por empresarios o particulares. No es solamente la A*imagen obscena en el Internet@*,tal como lo define *Makoto Ibusuki* (Prof. Univ. A.Kagoshima, Japón) entendiendo, por obscenidad como algo que: 1) estimula o exita el deseo sexual de las personas; b) ofende su sentido ordinario de vergüenza; y, c) está en contra de la moralidad sexual, según la Corte Suprema de 1951. Como ejemplos, se citan la publicación de novelas, fotografías y otros materiales impresos como digitales. En primavera de 1996, la corte encontró culpable por distribuir imágenes obscenas al público a través de las páginas WEB de internet, a Bekkoame, proveedor de las imágenes (art. 175 Código Penal). El caso Bekkoame, es el primero conocido en el Japón de pornografía en

internet. El distribuidor de esta imágenes, las recogió previamente en el extranjero y en los *newsgroups* para reproducirlas. Alrededor de 300 imágenes fueron observadas por más 100.000 usuarios de las páginas de Bekkoame desde diciembre de 1995. IBUSUKI, M. *LEGAL ASPECTS OF CYBER-PORN IN JAPAN.* En otras latitudes, en: ELMER-DEWITT, Phiplip. *INTERNET FIRE STORM ON THE COMPUTER NETS. A* new study of ciberporn, reported in a TIME cover story, sparks controversy. TIME Magazine. July 24, 1995 Vol. 146. Textos completos en WWW.UMONTREAL. EDU.CA.

el mundo del derecho, preocupantes, y a la vez candentes con el uso normal y corriente de las redes de información o datos de todo tipo, a través de *Internet* [179], que aún permanecen irresolutos, por lo menos en lo que más nos consta, es decir, en el ámbito del derecho público (Constitucional, Administrativo y penal), en donde todavía la teoría de los límites de derechos y valores constitucionales y legales, la sumisión de las nuevas tecnologías al derecho (informática vs. derecho), las reglas de ponderación y prevalencia de derechos y libertades públicas y la capacidad del Estado para proteger y reprimir conductas ilícitas informáticas, son paradójicamente determinables muros de contención para un océano o fenómeno global: Las redes de información o datos por vía informática o electrónica.

En efecto, los argumentos tan opuestos en estos temas están a la orden del día. Bástenos ver, como en los actuales momentos el derecho a permanecer en el anonimato en el *Leviatán* de las redes de información (internet), tiene preeminencia en el derecho, hasta tal punto que se plantean mecanismos de protección jurídicos y técnicos, como las llaves o claves públicas de encriptación de datos (Las Apublic-key encryption@, que se van extendiendo como mecanismos eficaces de protección de datos personales, y sobre todo en el sistema comercial y financiero. v.gr. La normativa específica sobre la Acriptologie symétric et asymétric@, en protección derechos y libertades públicas en sector financiero francés [180]) en combinación con un especial Aanonymous remailer@ en los computadores. Para ello, *es útil distinguir entre cuatro tipos de comunicación en que el remitente físico (o Areal@) puede esconder, al menos parcialmente, su identidad: a) El*

(179) Vid. Diario *LA VANGUARDIA.* Barcelona, Domingo, 1 de Marzo de 1998. Se realizan dos preguntas: 1)) Qué le preocupa más de internet?. Se responde: a) la Intimidad (30.49%), b) La censura (24.18%), c) La navegación (16.65%), d) Impuestos (8.93%), e) Encriptación (4.79%), f) Otros (14,96). 2) Debe haber nuevas leyes para proteger la intimidad?: a) Totalmente de acuerdo (39%), b) De acuerdo (33%), c) No le importa (11%), c) Totalmente en desacuerdo (7%), d) Más o menos en desacuerdo (7%). Fuente: The graphic, visualización & usability center´s (*WWW. BIANNUAL@USER.SURVEYS)*

(180) Vid. CAPRIOLI, Eric. *SÉCURITÉ TECHNIQUE ET CRYPTOLOGIE DANS LE COMMERCE ÉLECTRONIQUE EN DROIT FRANÇAIS.* Professeur Associé à l'Université de Nice - Sophia Antipolis. Sostiene: AEn général, on distingue la cryptogie symétrique où une clé identique est utilisée pour crypter et décrypter le (ou les) message(s) envoyé(s) et la cryptologie asymétrique qui utilise deux clés différentes. L'utilisateur distribue sa clé publique et il garde sa clé privée. Seules les personnes autorisées ont accès aux données transmises. Vis-à-vis de l'intégrité des données sur le message, c'est l'association d'une formule mathématique au message qui permet d'en garantir la teneur. La cryptologie permet de prévenir également contre le risque de répudiation des messages. Le plus célèbre système de cryptage, le logiciel "Pretty Good Privacy" (PGP),était pour l'instant interdit d'utilisation en France !@

anonimato identificable; b) Anonimato imposible de encontrar, c) El Seudo-anonimato; y d) El Seudo-anonimato identificable [181]. De otro lado, se sostiene que hoy , no debemos preocuparnos por el anonimato, cuando en el ciberespacio bullen por millones las páginas WEB (Word Wide *Web*) con datos personales y existe una amplia facilidad para accederlas por parte de terceros (hackers y/o crackers), e incluso por proveedores de acceso a la red. Igualmente, se sostiene que aunque teóricamente la LORTAD, protege a la intimidad de los cibernautas, los expertos consideran que es insuficiente, y que antes que termine 1998, se debería reformar la LORTAD adaptándola a las últimas recomendaciones previstas en las normas Comunitarias Europeas. Se estima en consecuencia, A)*que ni con leyes o sin ellas, internet marca la era del fin del anonimato?*@[182] (los signos de interrogación son nuestros). La reforma a la LORTAD que se plantea, podría venir, principalmente, por dos cauces: a) Por vía legislativa, y b) Por vía jurisprudencial una vez se resuelvan los varios recursos de inconstitucionalidad que pesan sobre la LORTAD, precisamente; entre otros fundamentos jurídicos, por rebajar los mínimo de protección y garantía de derechos como la intimidad, previstos en la Convenio Europeo de 1981, y por la adecuación de aquella a las recientes normas sobre tratamiento automatizado de datos personales y el sobre el flujo trans fronterizo de datos (Directiva 95/46/CE).

5.2.5.2. Medios informáticos físicos, en particular, los denominados de Ahardware@, como sistema informático de almacenamiento y tratamiento de datos[183]

(181) Vid. FROOMKIN, Michael. *ANONYMITY AND ITS ENMITIES*, 1995.Texto completo en: WWW.UMONTREAL.EDU. CA.

(182) Vid. A) Adiós al anonimato?@ En: Diario LA VANGUARDIA.Domingo, 1 de marzo de 1998.

(183) El término *hardware* ha sido aceptado por la Real Academia de la lengua Española, y su hermana, la Academia de la lengua colombiana. Vid. *GONZALEZ NAVARRO, F*. ***Comentarios a la ley...*** Ob.cit. pág.812. El Hardware, hace referencia a todos aquellos componentes materiales del ordenador o computador, conocido con el nombre genérico de equipo (puesto que consta de varios aparatos y dispositivos) y consta de unidades principales y periféricas. Las Unidades principales del Hardware, se dividen a su vez, así: a) *partes externas* (Unidad de sistema --chasis o armazón del ordenador con sus partes--, el teclado o consola y la pantalla de visualización --monitor o video); y, b) *partes internas* (tarjeta principal de circuitos, partes eléctricas, electrónicas y mecánicas. Aquí se encuentra la base principal de tarjeta principal de Chips y la caja de energía eléctrica, zonas de carriles y tarjetas electrónicas y las zonas de las unidades de disco flexibles y no removibles o fijas). Se incluye también los sistemas informáticos físicos que sirven para el almacenamiento, procesamiento, recuperación y transmisión de toda clase de información o datos, es decir, los conocidos o conocibles en el futuro. Dentro de los primeros están: a) Los Discos flexibles de acetato de 3 2 y 5 1/4 pulgadas. Pioneros formatos de almacenamiento que muy pronto fueron cambiados por los CD´s, aunque todavía se utilizan y cumplen su función con los actuales PC´s fijos o portátiles --notebook--; b) La gran familia de los CD´S --Compac Disck, de alta capacidad de almacenaje de datos, texto, imágenes, o todo a la vez, tales como los CD-ROM , CD-RAM, CD-I y DVD Disco Digital de Video; c) Los denominados ABackups@ o unidades de cinta, estilo cassette, para copias de seguridad en un sistema de procesamiento de datos de cualquier tipo. Un estudio más amplio en mi trabajo, *Constitución 1991 y la informática jurídica*... Ob. cit., pág. 128 a 234

Los medios informáticos físicos, en particular , los de hardware, son entonces, todos aquellos mecanismos, instrumentos, aparatos, elementos o sistemas físicos utilizados para el acceso, almacenamiento, tratamiento propiamente dicho de la informa-ción o datos de carácter automatizado (que incluye la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias), así como también, todos aquéllos equipos o aparatos asimilados a éstos y que utilicen un *chip* [184] *o microchip* en su unidad de procesamiento central (CPU) y cumplan iguales fines que los primeros. En la actualidad son tantos, tan variados y sofisticados estos medios informáticos físicos, que unidos con otros aparatos, instrumentos o elementos eléctricos, electrónicos o electromagnéticos utilizados en las tecnologías de la información y las comunicaciones TIC, conforman aparatos teleinformáticos o telemáticos que potencian sofisticadamente las funciones primarias de todos los ordenadores (tales como: la función de cálculo, la de tratamiento y conservación de la información, la de encadena- miento lógico y la de comunicación misma [185]), como el control tecnológico certero, sistemático, penetrante e indivisible tanto visual como auditivo de las personas [186].

De la unión de las telecomunicaciones [187] con los medios informáticos físicos tradicionales (El ordenador: procesador --CPU--, memoria, unidades de entrada y salida de información --E\S--, almacenamiento en Disco --fijo o móvil de variadas clases-- y unidades periféricas --E\S--), surge la teleinformática, pues Acualquier cosa que lleve un chip estará conectada internet (o a cualquier

---

(184) A título de ejemplo, el denominado *AChip antiviolencia@*, que ha producido polémica en los Estados Unidos, pues a partir del 2000, los ordenadores y televisores llevarán instalado el v-chip o chip antiviolencia, como un mecanismo de autocensura o autocontrol de imágenes, sonido y texto. El mecanismo para el televisor es prácticamente un mando de control a distancia que permite a los adultos apagar los aparatos que presenten películas consideradas perjudiciales para los niños o menores. En los ordenadores que son capaces de recibir imágenes, audio y video (como el WebTV), a través del internet, tal parece no van a ser instalados estos v-chip, pero sí en aquellos ordenadores que son capaces de recepcionar la señal de TV, común y corriente, previa la instalación de una tarjeta electrónica y dispositivos apropiados para tal fin, pues en este caso, el ordenador, es utilizado por la señal de TV, como un terminal de sonido e imagen, al prestar su estructura física, y en particular, su monitor, nada más. Vid. Diario *EL MUNDO.* Barcelona, Domingo, 22 de Marzo de 1998

(185) Mi trabajo, *LA CONSTITUCION....* Ob. cit. pág. 135

(186) MORALES PRATS, F. Ob. cit., pág.153

(187) Vimos, anteriormente (apartado5.5.3.2.2.), que existe una amplia gama de medios que utilizan las telecomunicaciones por ondas, cable o satélite, tales como la radiocomunicación y radiofusión, la telefonía básica, telex, telegrama, etc., así como los que se catalogan de Aservicios@ atendiendo a la actividad desarrollada (telefonía móvil, teletex, telefax, burofax y el datafax) y no a la técnica empleada.

Red de información o telecomunicación). Televisiones (entre ellas, la televisión digital por satélite, ya en funcionamiento), equipos de música y teléfonos celulares, entre otros (telefonía alámbrica, la televisión digital por satélite y sus aplicaciones v.gr. *Red 2000: canal temático sobre informática e internet en vía digital*) se comunicarán sin problemas con los ordenadores@[188], para transmitir, emitir o recepcionar señales de información, cualquiera sea ésta: texto, imagen, gráficos, sonido, o combinaciones de estos, y sea cual fuere el soporte que se utilice para grabar o recuperar la información o los datos emitidos o recepcionados.

En la última década [189], el empleo de los circuitos o sistemas cerrados de televisión (CCTV. A*Closed Circuit Television*@), inicialmente diseñados para la vigilancia y prevención del delito en centros de educación, bancarios, de salud, instituciones de toda clase, sitios de parqueo y edificaciones públicas y privadas, etc, ha crecido inusitadamente en el mundo y, especialmente, en las grandes ciudades de la Gran Bretaña, Norteamérica, Australia y varios países de Europa.

En efecto, estos mecanismos de almacenamiento, procesamiento y transmisión de información o de datos con imágenes digitalizadas fijas o en movimiento o de vídeo, fueron creados con fines de seguridad y prevención de la sociedad contra posibles actos delictivos. Esta forma de vigilancia se ha convertido en una especie de control social efectivo que refuerza el control policivo. Sin embargo, en la Gran Bretaña estas nuevas tecnologías han causado un gran impacto en la comunidad, más que ninguna otra, principalmente porque se ha visto involucrado la Intimidad (Aprivacy@) de las personas con profundos efectos para las generaciones futuras, tal

---

(188) Vid. Diario EL MUNDO. Barcelona, Domingo, 22 de Febrero de 1998.

(189) La AVideo Surveillance@, como industria en la Gran Bretaña, ha recibido entre 150 y 300 millones de libras, al instalar unas 300.000 cámaras para los sistemas de CCT, en diferentes sitios públicos y privados. Los diferentes impactos que ha ocasionado el adelanto técnico y sus constantes colisiones con los derechos fundamentales, se ha visto reflejado en los innumerables casos y escritos sobre el tema. v.gr. a) Testimonio del Director General Simon Davies ante la Cámara de los Lores, sobre la AVisual evidence and surveillance@, Oct. 23 de 1997. b) Perjuicios ocasionados por los dispositivos ACCTV Targets, KDIS On line@, Oct. 24/97; c) La APrivacy Internacional@ ha aplicado cuestionarios para evaluar los impactos de las CCTV (FAQ: Frequently Asked Questions); d) Reales amenazas mundiales con los sistemas de vigilancia CCTV. Los sistemas de video y transmisión de imágenes con cámaras ocultas y otros dispositivos, etc. Texto completo en WWW.UMONTREAL.EDU.CA.

como lo ha expresado la Oficina de la APrivacy Internacional@ [190]. Impactos que ya se están observando, pues los sistemas de CCTV unidos a la informática (principalmente en el almacenamiento y tratamiento de información digitalizada y/o video), hoy han potenciado su actividad y riesgo frente a los derechos y libertades de la persona.

El Soporte, según el art. 3, a) del R.D. 263/1996, *es el objeto sobre el cual o en el cual es posible grabar y recuperar* información o datos de todo tipo. Desde el punto de vista de la informática, el soporte constituye el dispositivo idóneo en el cual se puede almacenar, tratar y recuperar información análoga o digitalizada. v.gr. los discos magnéticos no removibles o fijos (discos mal llamados *duros*) y la variopinta clasificación de los discos flexibles o removibles: a) discos de acetato: Discos de 3 2 y 5 1/4 pulgadas, b) la familia de los discos compactos (*Compac Disc*) que aumentó ostensiblemente la capacidad, la versatilidad del disco de acetato y potenció el almace namiento y recuperación de información de texto, gráfica, auditiva y visual. Entre los más importantes, están: El típico CD, CD-ROM --sólo lectura--, CD-RAM -- lecto- escritura-- CD-I -- audio, video e interactivo y el DVD --Disco Digital de Vídeo o Disco digital versátil-- que supera en siete veces la capacidad de su predecesor CD, y c) Los denominados ABackups@ o unidades de cinta, estilo cassette, para copias de seguridad en un sistema de procesamiento de datos de cualquier tipo, corrientemente utilizados en el sector comercial y financiero, privado y público, para salvaguardar grandes cantidades de información o datos, almacenados y organizados en forma diaria, mensual o anualmente o por sistemas de ordenación utilizados en la estadística o las ciencias matemáticas o sociales.

El Tribunal Supremo Español reiteradamente ha explicado qué debemos entender por documento informático acudiendo a la técnica de la asimilación de los requisitos generales y especiales del documento *lato sensu* y, a la ejemplificación de los elementos, dispositivos,

---

(190) AVideo Surveille@. Texto en *WWW.UMONTREALEDU.CA*. La sede principal de la Oficina por el derecho a la Intimidad esta en la Gran Bretaña. Esta Oficina se ha constituido como una institución con ámbito global, con especial énfasis en los países de la Common Wealth, para la defensa de la Intimidad, sea cual fuere los mecanismos, instrumentos o equipos o aparatos de la tecnología TIC en unión con la informática, que se utilicen como posibles medios (mecánicos, eléctricos, electromagnéticos visuales o audio-visuales) para la comisión de un delito o infracción de carácter administrativo.

aparatos o equipos de computación (componentes del hardware), así como a la nominación de los programas de ordenador (software).

En efecto, se sostiene que documento es

> el escrito, en sentido tradicional, *o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un disquete, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como *cualquier cosa que sirve para ilustrar o comprobar algo+ (obsérvese que se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el aplicador del derecho tener en cuenta la evolución social), siempre que el llamado *documento+ tenga un soporte material, que es lo que sin duda exige la norma penal* (por todas, TS SS 1114/1994 de 3 Jun., 1763/1994 de 11 Oct. y 711/1996 de 19 Oct.). **[191]**

Sin embargo, Aun disquete@ o cualquier otro dispositivo que se utiliza para almacenar, procesar o transmitir información *per se* no es un documento, sino un elemento que puede contenerlo. Lo especial del dispositivo es que es un mecanismo electrónico o electromagnético con estructura radicalmente diferente a otros soportes tradicionales de los documentos como el papel, pero nada más. La estructuración del documento informático se da sólo cuando reúne los requisitos de forma y de fondo previstos en el ordenamiento jurídico para ser un *documento*, en general, y cuando los medios, equipos, aparatos y soportes en los que se ha almacenado, procesado o transferido la información o datos específicos a cierto *negocio jurídico* o actividad personal, comercial o financiera , etc., son catalogados de informáticos (hardware y software), electromagnéticos o telemáticos (v.gr. *documento EDI* --Electronic Data Interchange--, utilizado en transacciones públicas y privadas de carácter económico, financiero, laboral o administrativo[192], Amensajes de correo electrónico@ --E-Mail--, y los A*PAGER@* de E-Mail --Busca personas electrónico: texto, sonido e incluso imagen-).

---

(191) STS Nov. 23 de 1996. M.P. Montero Fernández. FJ. 6.A. Cfr. AA.VV. Compendio discos Aranzadi. Ob. cit., Madrid, 1997.

(192) También conocido documento de intercambio electrónico AIED@. Se estructura por que el formato debe ser normalizado y la conexión se realiza entre ordenadores o computadores. En España este tipo de documentos se utiliza en transacciones privadas y públicas comerciales y administrativas de carácter tributario, según la Ley de 28 de diciembre de 1992 que regula el Impuesto de Valor Añadido.IVA. ,art. 88.2 y el RD. 2402/1985, 29 de diciembre de 1992, art. 4).

La identificación del dispositivo o soporte con la clase del documento al que se quiere referir (papel para el documento *escrito-tradicional* y variadísimos elementos, dispositivos, sistemas o aparatos eléctricos, mecánicos o electrónicos para los documentos *no escritos-asimilados* en su variopinta clasificación y dentro de esta los denominados *informáticos o electrónicos*) es factible a los efectos de continente o recipiente y de la posibilidad de disponer o no de las nuevas tecnologías TIC y la informática, pero no para la determinación del contenido mismo del documento ni mucho menos para determinar la clase de negocio jurídico contenido en este.

Los soportes informáticos contienen información o datos generales o específicos en discos electromagnéticos removibles o flexibles (uno de ellos los Adisquetes@), en cintas de backup, discos fijos o removibles y discos compactos (CD´s), en los cuales el mensaje se consigna mediante *magnitudes físicas que representan en forma codificada unas nociones o noticias y son susceptibles de registro, proceso y transmisión.* [193].

La referencia del C.P.Esp., en el art. 197.2, a los datos de carácter personal o familiar de hallarse registrados en ficheros (programas de computador) o soportes infor- máticos, electrónicos o telemáticos (elementos, aparatos o sistemas componentes de hardware principal y periférico), destaca al concepto *Asoporte@* como dispositivo o elemento continente de información y no contenido en sí mismo, a la luz del artículo 3, a) del R.D. 263/1996, que cataloga al soporte como el objeto en el cual es posible grabar y recuperar información; pero también hace alusión a la posible clasificación antes doctrinal, hoy legislativa de *documento informático, electrónico o telemático*, empleado por las leyes administrativas en el art. 37 y 45 de la LRPA., y que sirven de normas extrapenales y interpretación del C.P.Esp. [194] . Sin embargo, en este aparte nos referimos
al conjunto de elementos de hardware o software como medios informáticos en la comisión de una

---

(193) Vid. HEREDERO HIGUERAS, M. *VALOR PROBATORIO DE LOS DOCUMENTOS ELECTRONICOS.* Citado por GONZALEZ NAVARRO, F. Comentarios a la ley.... Ob. cit., pág. 818.

(194) Véase, aparte 5.5.1, d), parte IV y Parte III, sobre el documento informático, electrónico o telemático.

conducta ilícita, es decir, como soportes o dispositivos informáticos o telemáticos capaces de almacenar y procesar información y ser objeto de Aapoderamiento, utilización, modificación@ (o accesión) o ser Aalterados@ (procesados o tratados) informática o electrónicamente.

5.5.2.3. Medios informáticos lógicos, en particular los denominados de Asoftware@. El Afichero@, como programa de ordenador.

La Directiva 95/46/CE, en sus considerandos 20, 26 y 63 hace referencia a la calidad, oportunidad o necesariedad, razonabilidad y efectos de protección de los medios utilizados en el procesamiento, almacenamiento y transferencia de información o datos. Estos no deberán obstaculizar ni el procedimiento del tratamiento automatizado, propia mente dicho, ni mucho menos, los principios de protección de las personas identificadas o identificables. Para mantener un equilibrio entre la utilización y la obstaculización que los medios pueden ocasionar, *hay que considerar el conjunto de los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier persona* en el transcurso de un tratamiento automatizado de datos, el cual deberá *regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la Directiva.* Aunque la referencia a los medios es genérica (jurídicos, técnicos y legislativos), consideramos a nuestros propósitos, que pueden ser aplicados perfectamente a los medios informáticos.

En efecto, el R.D. 263/1996, expresa que cuando *utilicen los soportes, medios y aplicaciones, se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confiabilidad, integridad, disponibilidad y conservación de la información.* (art. 4.2). Estos principios de protección de los medios y demás elementos y dispositivos informáticos, electrónicos y telemáticos garantizan el uso legítimo de los mismos por parte de la Administración General del Estado y sus entidades de derecho público, y obviamente, los derechos e intereses legítimos de los particulares o ciudadanos.

No en vano, se expresa que entre las medidas de seguridad aplicadas a los soportes, medios y aplicaciones utilizadas, la Administración y las entidades de derecho público deberán garantizar: a) la restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas, b) la prevención de alteraciones o pérdidas de los datos e informaciones y c) la protección de los procesos informáticos frente a manipulaciones no autorizadas.

Esta plataforma de garantías sobre la utilización se refiere a los medios informáticos en general, aunque la norma citada denomina Aaplicación@ al software [195], consideramos a éste como un medio informático lógico o logicial, sin importar su calificación o la pretendida castellanización del término para mejor entendimiento del lector jurídico. En efecto, se entiende por Aaplicación@, *el programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el recurso a un sistema de tratamiento de la información.* La conceptualización abarca, a la vez, el significante (software) y el significado (definición), para decir que éstos tienen como objeto la solución a un problema, no sin actuar con otros recursos ( )cuáles?.Se entendería lógicamente, los de hardware) para llegar al verdadero fin: el tratamiento automatizado de la información. Por ello, hubiese sido mejor conceptualizar qué se entiende por programa o software, antes que conducir al error interpretativo del operador jurídico con la aptitud tomada por Real Decreto, al unificar los conceptos de software y hardware como uno sólo. Bien es cierto que para un procedimiento automatizado se requiere ineludiblemente el concurso de ambos, pues las tareas del ordenador se llevan a cabo por la fusión estructural y de procesamiento lógico de uno y otro; no es menos cierto, que cada cual tiene su propia identificación y conceptualización en el ámbito de la protección jurídica [196], aunque más acentuada y protegida por los estados del mundo para el Software (desde propuesta internacional de la OMPI --Organización Mundial de Propiedad

---

(195) El anglicismo *Software (soft* -Ablando@- y *ware* -Aartículos manufacturados@-) ha ingresado a todos los idiomas, sin necesidad de traducción literal o interpretativa del término, quizá por ser más explicativo éste que las traducciones mismas. La traducción castellana del software más comprensible ha sido de programa informático.

(196) La decisión de la multinacional IBM de realizar facturación separada para los productos de hardware y por productos de software, produjo en los años 60´s, la separación de los estos componentes del ordenador, a la vez que incentivó los múltiples intentos de buscar una protección jurídica adecuada para los programas de ordenador. Esta decisión, tomada por IBM, vino forzada por las medidas impuestas por el Departamento de Justicia de los Estados Unidos para evitar la monopolización de un determinado mercado y la aplicación de unas normas para obviar la competencia desleal. Véase, también en:. DAVARA RODRIGUEZ, Miguel. *MANUAL DE DERECHO INFORMATICO*. Ed. Aranzadi, Pamplona, (Esp.), 1997, pág. 103. En 1993, la Ley 16/1993 de diciembre incorpora al Derecho español la Directiva 91/250/CEE, de 14 de mayo, sobre la protección jurídica de los programas de ordenador. En Colombia, la protección jurídica al software encuentra abrigo en *La propiedad intelectual (art.61 Cons.Col):* derechos de autor (Ley 23/32, Ley 44 /94 y D.R.1983 de 1991) y, en particular, la protección al soporte lógico o Asoftware@ (Dec.1360 de Junio 23 de 1989).

Intelectual-- de 1977), a través de los derechos (morales y patrimoniales) y deberes que genera la protección intelectual, antes que para el hardware que constituye el chasis estructural movido por la energía y sustancia central y periférica, llamada software, pero al fin y al cabo identificables por separado.

No en vano se ha dicho que las *autopistas o la sociedad de la información son el resultado de la confluencia de diversas tecnologías: la digitalización, los programas de ordenador y las redes de transmisión de banda ancha* [**197**], compuestas por una serie de equipos y sistemas estructurales informáticos puestos en funcionamiento para que produzcan resultados, con la predisposición necesaria e ineludible de otros llamados programas o soportes logiciales, que hacen posible las tareas de tratamiento automático de cualquier tipo de información.

Por tanto:)Qué entendemos por un programa de ordenador?. Programa de ordenador es *toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una tarea u obtener un resultado determinado, cualquiera que fuera su forma de expresión y fijación@* (art. 96 de la Ley de Protección de la Propiedad Intelectual Española, LPI). La protección jurídica en la LPI, se extiende no sólo al software concluido, sino también a los contenidos en las diferentes etapas de elaboración y los diversos componentes, a saber: a) Códigos fuente y objeto (la versión del programa accesible únicamente a la máquina, es decir, el lenguaje en el que está escrito); b) Programas de explotación y de aplicación (es decir, el sistema base que controla las funciones internas de los ordenadores o facilita su uso y la aplicación respectiva); c) Algoritmos (conjunto de pre-escrito de reglas o instrucciones bien definidas para la solución de un problema), d) Material preparatorio (documentación preparatoria del programa: texto, gráficos, diseños, etc), e) Interfaces y componentes visuales del programa (partes que permiten la interconexión e interacción entre los

---

(**197)** Vid. BERCOVITZ, Alberto. *Riesgos de las nuevas tecnologías en la protección de los derechos intelectuales. La quiebra de los conceptos tradicionales del derecho de propiedad intelectual. Soluciones prácticas.* En: El Derecho de Propiedad Intelectual... Ob. cit., pág. 71.

elementos del software y hardware, es decir, los elementos lógicos destinados a gestionar la comunicación entre el sistema y el usuario o entre sistemas. Los componentes visuales como los screen displays o imágenes-pantalla); y f) Documentación técnica y manuales de uso (por la asimilación de programas de ordenador a obras literarias, siguiendo las recomendaciones internacionales v.gr. Directiva 91/250/CEE, de 14 de mayo) [198].

Esta amplia y extensiva gama de protección jurídica civilista e iusadministrativista del software en la LPI, como *prima ratio,* hoy más que nunca, evidencia el arsenal jurídico que todos los Estados [199], como España (a través de la LPI y otros instrumentos normativos y Apor otros derechos@ [200]: a) Derecho de patentes, LP 11/1996; b) Derecho de marcas, LM 32/1988; c) Código Civil (arts.1091, 1101, 1106, 1255, 1257; d) Estatuto de Propiedad industrial, EPI), anteponen de forma ultraprotectora frente a la protección jurídica penal o de *ultima ratio.* En efecto el C.P.Esp., dedica una protección penal expresa del software en el Título XIII, Deli-
tos contra el Patrimonio: Cap. IX, De los Daños (art. 264.2) y el Cap. XI, Delitos relativos a la propiedad intelectual e Industrial, (art.270 y ss.), así como también en forma extensiva e interpretativa en el Cap. I, del Título X, Delitos contra la intimidad, puesto que se reprime las conductas realizadas con medios informáticos (hardware o software) que atenta a la intimidad de las personas, y sobre todo cuando hace énfasis en el término *Afichero@.*

Ahora bien: Sí los ficheros automatizados o bancos de datos, son *todo conjunto organizado de datos de carácter personal que sean objeto de tratamiento automatizado, cualquiera que fuere*

---

(198) Este ámbito de protección corresponde a las *Categorías de programas protegidos por la LPI*, art.1, punto 2, 4 y 96. CERCOS PEREZ, Ramiro. *PROTECCION JURIDICA DE LOS PROGRAMAS DE ORDENADOR.*. En: Ambito jurídico de las tecnologías de la información. Revista C.S.J.P. Núm., XI, Madrid, 1996, p. 107 a 111.

(199) Las presuntas prácticas monopolistas y de competencia desleal entre los productores mundiales de sof ware de AMicrosoft de --Williams- Bill Gates@, por la salida al mercado de su software AWindows 98", que incluye en su programa ambiente, de ventanas y operativo, un programa o sistema de intercomu-nicación entre ordenadores, a través de redes de información, una especie de navegador por el ciberespacio. Aunque el *Explorer de Microsoft,* como el *Netscape de Barksdale,* realizan estas actividades actualmente y por separado de los programas operativos de un ordenador. El caso de Microsoft con su *Windows 98,* no es igual porque éste fusiona el programa operativo de ventanas especial (Windows 95) a un simil de *Explorer* avanzado técnica como funcionalmente. Esta fusión obliga al comprador o usuario de Windows 98 a utilizar el programa operativo con el programa intercomunicador o de transferencia de datos. La obra colectiva del programa de ordenador denominado *Windows 98,* que pertenece al empresario Bill Gates, demanda ante los Tribunales Norteamericanos por Barksdale de NETSCAPE y el apoyo de ORACLE (Empresa de sistema de Red), por actividades presuntamente

monopolísticas y de competencia desleal, al perder mercado las empresas que actualmente y en forma independiente tienen la oferta y demanda de los programas de computadores conocidos como navegadores de las redes de información. Más al respecto, en DIARIO *EL MUNDO, Domingo*, Mayo 24 de 1998, pág.11 y 12.

(200) Vid. CERCOS PEREZ, R. Ob. cit., págs. 127 a 133.

la forma o modalidad de su creación, almacenamiento, organización y acceso, y éstos pueden ser objeto de *operaciones y procedimientos técnicos, de carácter automatizado, 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* (LORTAD, art. 3, b), y c),), se concluye, sin lugar a dudas que el término Afichero@, utilizado por el art. 197.2. del C.P.Esp., es considerado, a la luz de la infor- mática, como un programa de ordenador, puesto que como todo programa de ordenador facilita o complementa un conjunto de operaciones, instrucciones, tratamientos y *comunicación de datos o informaciones del hombre con la máquina en forma automatizada, o entre ordenadores* en forma electrónica o telemática. En efecto, todas las actividades relacionadas en el art. 3, con los ficheros son funciones y atribuciones propias de los programas de ordenador a las cuales tienen acceso, tanto el hombre (STC 328/1998, Enero 1. FJ.4, A*programa informático@*) como el ordenador mismo.

Estos ficheros o programas de ordenador, en términos del C.P.Esp., Tít.X,Cap.I y la LORTAD, contienen datos o informaciones de carácter particular o familiar, si se refieren a informaciones de personas físicas identificadas o identificables (art.3, a,), que es objeto de protección jurídica, bien se trata ficheros de carácter público o privado, de autoría individual o colectiva **[201]**, sí utilizan o no los nuevos recursos de la tecnología TIC y la informática v.gr. las redes informáticas de multimedia, si los utilizan; o en fin, sí han sido, a su vez, creados, organizados y puestos a funcionamiento, mediante un determinado lenguaje de programación (considerado también, un programa de ordenador, v.gr. Pascal, Cobol, Fortran, etc) o a través de gestores de bases de datos (como p.e. DBase) o de programas de creación o manejo de hipertexto o páginas WEB en redes informáticas (v.gr Java en internet). Lo que sí determinan estas últimas conclusiones es que los programas de ordenador en términos de la normatividad penal y extrapenal

(201) Los programas de ordenador tienen como autor a una persona natural determinada, y por tanto, los derechos morales y patrimoniales le corresponden a éste. Sin embargo, en no pocas veces la obra es contratada (relación laboral) en su realización por un empresario determinado. En este caso, la autoría de la obra le corresponde a una persona natural individual o colectivamente considerada, en tanto que los derechos patrimoniales le pertenecen al empresario, quien es su titular. Vid. BERCOVITZ, Alberto. *Riesgos de las nuevas*... Ob. cit. pág. 79

española referida a los datos de carácter personal y familiar se pueden clasificar, así: a) por la finalidad u objeto perseguido: aplicativos y/o de servicios; b) por la autoría: individuales y colectivos; y c) por la titularidad: públicos y privados.

En tal virtud, un programa de ordenador que contiene, maneja, administra o transfiere datos o informaciones de carácter personal y al cual se puede acceder, modificar, cancelar o borrar registros y consultar, en general, de forma autorizada, vista la informática jurídica y con base en la clasificación general del software [202], se puede catalogar de un programa de ordenador de carácter aplicativo, de servicios, de comunicación, acceso y sistemas informáticos. Sin embargo, por ahora, no es el objeto de este trabajo, pormenorizar sobre estos tópicos, sino apenas referenciales para ver la magnitud del término, del significante y significado llamado *fichero* y su lícita e ilícita utilización en la legislación ibérica.

También interesa destacar, por el momento, que los programas de ordenador, son: de un lado, un medio informático comisivo potente, penetrante, certero e intangible para ejecutar y consumar delitos contra la intimidad; y de otro, un objeto de protección jurídico penal, cuando se reprime conductas realizadas con programas de computador por cualquier persona no autorizada para acceder, utilizar o alterar datos o informaciones de carácter personal o familiar.

---

(202) Con base en el Decreto 260 de 1980, reglamentario de la Ley 13/1996, clasificamos los programas de ordenador o computador, así: a) *Los programas operacionales*, que permiten el funcionamiento y control del ordenador; b) *Los lenguajes de programación*, que facilitan el desarrollo de los programas, en general; c) *Los programas aplicativos*, proporcionan soluciones específicas a problemas de manejo de datos de todo tipo; d) *Los programas de servicios desarrollados para propósitos específicos*; manejo de datos o informaciones, accesibles y consultables por personas autorizadas con fines predeterminados; e*) los sistemas de programación*, que manejan y administran bases de datos, en general: *f) Los programas de soporte*, facilitan la interacción de equipos de procesamiento de datos y la administración de redes de comunicación para la transmisión de intercambio de información codificada o decodificada; g) *los programas de comunicación y acceso a base de datos externas a una entidad*, y h) Otros, dentro de los que se encuentran todos aquellos programas que se producen, día a día, por la tecnología, se catalogan como *software*, se utilizan en el sistema de información automatizada y no están previstos en las anteriores categorías. Véase, Mi trabajo, *LA CONSTITUCION Y LA INFORMATICA*....Ob. cit., págs 199 y ss.

BIBLIOGRAFIA GENERAL

[*AA.VV.*, 1997]

AA.VV. A***Base de datos Acelex@.*** Ed. Comunidad Europea, Bruselas, (B), 1997.

[*AA.VV.*, 1997]

AA.VV.***AColección de Discos Compactos: Jurisprudencia del Tribunal Constitucional y Tribunal Supremo Español@.*** Ed. Aranzadi, S.A., Pamplona, 1980-1997.

[*AA.VV.*, 1997]

AA.VV. ***AColección de Discos Compactos: legislación española y comunitaria@. E***d. Aranzadi, S.A., Pamplona, 1930-1997.

[*AA.VV.*, 1997]

AA.VV. ***AColección de Discos Compactos: jurisprudencia del Tribunal Constitucional y Tribunal Supremo Español.*** Ed. Colex, S.A., Madrid, 1997.

[*AA.VV.*, 1997]

AA.VV. ***AColección de Discos Compactos: legislación española y comunitaria@. E***d. Colex, S.A., Madrid, 1997.

[*AA.VV.*, 1997]

AA.VV. ***AColección de Discos Compactos de Legis, s.a.: a) Constitución Política de Colombia de 1991 -- legislación, jurisprudencia y doctrina--; b) Código Penal; c) Código Civil; y, d) Código de Comercio@.*** Ed. Legis, S.A., Santafé de Bogotá, 1997.

[*AA.VV.*, 1997]

AA. VV. ***AConstitución Política de Colombia@***. Ed. Legis, S.A., Santafé de Bogotá, edición de entregas en hojas sueltas, 1997.

[*AA.VV.*, 1997]

AA.VV. ***AConstitución Española@***. Segunda edición actualizada, Editorial, Civitas, Madrid, 1997.

[*AA.VV*., 1997]

AA. VV. ***AComentarios a la Constitución Española de 1978"***. Dirigida por Oscar Alzaga Villaamil, Tomo II, Arts. 10 a 23. Editoriales de Derecho Reunidas. EDERSA, Madrid, 1997.

[*AA.VV*., 1997]

AA. VV. ***ACódigo Nacional de Policía***. Ed. Ediciones lito imperio, santafé de Bogotá, 1997.

[*AA.VV*., 1997]

AA.VV. ***Código Penal. Doctrina y jurisprudencia.*** Tomo II, Artículos 138 a 385. Dirección: Cándido Conde-Pumpido F., Ed. Trivium, S.A., 1a ed., Madrid, 1997.

[*AA.VV*., 1997]

AA.VV. ***Código Penal y legislación complementaria@***. Vigésimo tercera edición actualizada a Septiembre de 1997, Editorial, Civitas, Madrid, 1997.

[*AA.VV*., 1996]

AA.VV. A***Ambito jurídico de las tecnologías de la información@***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J.No. XI, Madrid, 1996.

[*AA.VV*., 1996]

AA. VV. ***Código Penal y leyes penales especiales***. Coordinación y notas José Manuel VALLE MUÑIZ . Edición actualizada, Septiembre, Ed. Aranzadi, Pamplona (Navarra), 1996.

[*AA.VV*., 1994]

AA. VV. ***El EDI (Electronic Data Interchange***). En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*AA.VV*., 1992]

AA.VV. ***Informática e Intimidad.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 2 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1992.

[*AA.VV*., 1992]

AA.VV. ***Introducción a la informática (II).*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 2 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1992.

[*AA.VV*., 1982]

AA.VV. ***AConstituiçao novo texto@***. Ed. Coimbra. Ediçao organizada JJ. Gomes Canotilho o Vital Moreira, Portugal, 1982.

[*Arroyo*,1996]

ARROYO ZAPATERO, Luis. ***La intimidad como bien jurídico protegido***. En: Estudios de Derecho Judicial. Escuela Judicial. AEstudios Sobre el Código Penal de 1995. Parte Especial@. C.G.P.J., Madrid, 1996.

[*Arroyo*,1994]

ARROYO ZAPATERO, Luis. ***Actualidad político criminal del derecho penal económico en españa***. En: Estudios de Derecho Penal Económico. Editores Luis A. Zapatero y Klaus Tiedemann. Ed. Univ. De Castilla-la Mancha, Tarancón (Cuenca), 1994.

[*Arus*, 1996]

ARUS, Francisco B. ***Libertad de expresión y administración de justicia.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J.@Estudios sobre el Código Penal de 1995@. XI, Madrid, 1996.

[*Arus*, 1994]

ARUS, Francisco B. ***El delito informático***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 11 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Bacigalupo*, 1989]

BACIGALUPO ZAPATER, E. ***)Necesita el derecho español un delito de indiscreción?.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No.15, Madrid, 1989.

[*Bajo*, 1982]

BAJO FERNANDEZ, M. ***Protección penal del honor y de la intimidad.*** En: Comentarios a la Legislación Penal, T.I., Madrid, 1982.

[*Barnes*, 1997]

BARNES VASQUEZ, Javier. ***La internet y el derecho. Una nota acerca de la libertad de expresión e información en el espacio cibernético.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. AOrdenación de las telecomunicaciones@. Consejo General del Poder Judicial. C.G.P.J. No. VI, Madrid, 1997.

[Baon, 1996]

BAON RAMIREZ, Rogelio. ***Visión de la informática en el nuevo Código Penal***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Betes*, 1997]

BETES DE TORO, Alfredo. ***El derecho de información y los principios legitimadores del tratamiento automatizado de los datos de carácter personal en la Directiva 95/46/CE, de 24 de octubre de 1995.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 25 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Cabanillas*, 1994]

CABANILLAS MUGICA, Santiago. ***Introducción al tratamiento jurídico de la contratación por medios electrónicos (EDI) -- Electronic Data Interchange--*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Casenave*, 1996]

CASENAVE RUIZ, José. ***La protección jurisdiccional en el ámbito civil del programa de ordenador***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 19 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996.

[*Cueva*, 1994]

CUEVA CALABIA, José Luis. ***La LORTAD y la seguridad de los sistemas automatizados de datos personales***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 13 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Cano*, 1995]

CANO I ARTEROS, Silvia. ***La intimitat corporal, segons la jurisprudéncia del tribunal constitucional***. En: Revista Jurídica de Catalunya. R J.C. Núm. 4, Ed. Col.legi de Jurisprudéncia i legislación de catalunya. Director: Josep M. Vilaseco i marcet, Barcelona, 1995.

[*Carrascosa*, 1996]

CARRASCOSA GONZALEZ, Javier. ***Propiedad intelectual y derecho internacional privado español: perspectiva general***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 19 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996.

[*Carbonell*, 1996]

CARBONELL MATEU, J. C., y GONZALEZ CUSSAC. ***Comentarios al Código penal de 1995.*** Vol. I. Ed. Tirant lo Blanch, Valencia (Esp.), 1996.

[*Castells*, 1994]

CASTELLS ARTECHE, José Manuel. ***Derecho a la privacidad y proceso informáticos: análisis de la ley orgánica de 5 de 1992, de 29 de octubre de 1992 (LORTAD***). En: Revista Vasca de Administración Pública. R.V.A.P. Núm. 39, Bilbao (Esp.), 1994.

[*Castells*, 1991]

CASTELLS ARTECHE, José Manuel. ***la intimidad informática***. En: Estudios sobre la Constitución Española en Homenaje al Prof. Eduardo García de Enterría. Ed. Civitas, Tomo II., Madrid, 1991.

[*Cercos*, 1996]

CERCOS PEREZ, Ramiro. ***Protección jurídica de los programas de ordenador.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Chinchilla*, 1997]

CHINCHILLA MARTIN, Carmen. ***El régimen jurídico de las telecomunicaciones. Introducción.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. @Ordenación de las telecomunicaciones@. Consejo General del Poder Judicial. C.G.P.J. No. VI, Madrid, 1997

[*Clement*, 1996]

CLEMENT DURAN, Carlos y PASTOR ALCOY, Francisco. ***El nuevo y el viejo Código Penal comparados por articulos.*** Ed. General del Derecho, S.L., 3a ed., Valencia, 1996

[*Cobo*, 1997]

COBO DEL ROSAL, Manuel. ***Derecho penal español. Parte Especial II.*** Ediciones jurídicas y sociales, S.A., Madrid, 1997.

[*Correa*, 1988]

CORREA, Carlos María. ***Informatica y derecho***. Ed. Depalma. Buenos Aires, 1988.

[*Cueva*, 1994]

CUEVA CALABIA, José Luis. ***La LORTAD y la seguridad de los sistemas automatizados de datos personales***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 13 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Cremades*, 1995]

CREMADES, Javier. ***Los límites de la libertad de expresión en el ordenamiento jurídico español***. Ed. Ley-actualidad, Bilbao, 1995.

[*Cuchi*, 1996]

CUCHI DENIA, Javier Manuel. ***La libertad de información versus el derecho al honor:) De la técnica de la ponderación a la prevalencia de la primera?***. En: Revista General de Derecho. R.G.D. Núm.61., Valencia (Esp.), 1996.

[*Davara*, 1997]

DAVARA RODRIGUEZ, Miguel Angel. ***Manual de derecho informático.*** Ed. Aranzadi, (Navarra), Esp., 1997

[*Davara*, 1994]

DAVARA RODRIGUEZ, Miguel Angel. ***La protección de datos en España: principios y derechos***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 13 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*De carreras*, 1996]

DE CARRERAS SERRA, Lluis. ***Régimen jurídico de la información: periodistas y medios de comunicación.*** Ed. Ariel, Barcelona, 1996.

[*De la Serna*..., 1997]

DE LA SERNA BILBAO, María Nieves. ***La Agencia de protección de datos española: con especial referencia a su característica de independencia***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 22 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Dumortier*, 1996]

DUMORTIER, J. y ALONSO BLAS, Diana M. ***La transposición de la Directiva de protección de datos.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 20 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1996

[*Fairen*, 1996]

FAIREN GUILLEN, Víctor. ***El habeas data y su protección actual surgida en la Ley española de informática del 29 de Octubre (Interdictos, Habeas Corpus) --Primera Parte--***. En: Revista de Derecho Procesal, R.D.P. No. 3, Madrid, 1996.

[*Fariñas*, 1983]

FARIÑAS MATONI, Luis M. ***El derecho a la intimidad***. Ed. Trivium, Madrid,1983

[*Fernández*, 1997]

FERNANDEZ-MIRANDA, Alfonso y GARCIA SANZ C., Rosa María. ***Artículo 20.*** En: Comentarios a la Constitución Española de 1978. Dirigida por Oscar Alzaga Villaamil, Tomo II, Arts. 10 a 23. Editoriales de Derecho Reunidas. EDERSA, Madrid, 1997.

[*Fernández*, 1993]

FERNANDEZ CALVO, Rafael. ***Datos personales: tecnología, ley y ética.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 8 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1993.

[*Frosini*, 1988]

FROSINI, Vottorio. ***Informática y derecho***. Ed. Temis, Bogotá, 1988.

[*Frosini*, 1978]

FROSINI, Vittorio. ***Cibernética, derecho y sociedad***. Ed. Tecnos, Trad. de Carlos A. Salguero-Talavera y Ramón L. Soriano Díaz, Madrid, 1978.

[*Gallardo*, 1996]

GALLARDO ORTIZ, Miguel Angel. ***informartoscopia y tecnología forense***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Garberi*, 1994]

GARBERI LLOBREGAT, José. ***La Audiencia Nacional y el enjuiciamiento de los delitos económicos***. En: Estudios de Derecho Penal Económico. Editores Luis A. Zapatero y Klaus Tiedemann. Ed. Univ. De Castilla-la Mancha, Tarancón (Cuenca), 1994.

[*García...*,1996]

GARCIA DE ENTERRIA, Eduardo y FERNANDEZ, Tomás-Ramón. ***Curso de Derecho Administrativo.*** Tomo I, 7a., ed., reimpresión 1996 y Tomo II, 4a., ed., Civitas, reimpresión 1995, Ed. Civitas, Madrid, 1995-1996.

[*Gardarin*, 1989]

GARDARIN, Georges. ***Bases de donnés. Les systems et leurs langages.*** Editions Eyrolles, París (F), 1989.

[*Gimeno*, 1997]

GIMENO SENDRA, Vicente. ***Derecho a la intimidad física y a la intimidad personal.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 278 de 23 de enero, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Giraldo*, 1985]

GIRALDO ANGEL, Jaime. ***Metodología y técnica de la investigación jurídica***. 30 ed., Ed.Librería del Profesional, Bogotá, 1985.

[*Giraldo*, 1985]

GIRALDO ANGEL, Jaime. ***La metodología de la investigación jurídica aplicada a la elaboración del documento jurisprudencial para informática***. Revista Universidad Pontificia Bolivariana de Medellín.No.68, Medellín, 1985

[*González*, 1997]

GONZALEZ NAVARRO, Francisco y GONZALEZ PEREZ, Jesús. ***Comentarios a la ley de régimen jurídico de las administraciones públicas y procedimiento administrativo común. (Ley 30 de 1992).*** Ed. Civitas, 1a., ed, Madrid, 1997.

[*González*, 1994]

GONZALEZ QUINZA, Arturo. ***Recurso de amparo sobre el acceso a ficheros públicos automatizados de carácter personal. Caso AOlaverri"*** . En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*González*, 1992]

GONZALEZ-TREVIJANO SANCHEZ, Pedro José. ***Los derechos fundamentales y libertades públicas en la Constitución colombiana de 1991.*** En: Revista de Derecho Político. R.D.P. Núm. 35. Univ. Nacional de Educación a Distancia. UNED. Madrid, 1992.

[*González*, 1992]

GONZALEZ SEGADO, Francisco. ***El Sistema Constitucional Español***. Ed. Dykinson, Madrid, 1992.

[*Gutiérrez*, 1996]

GUTIERREZ FRANCES, María Luz. ***Delincuencia económica e informática en el nuevo Código Penal***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Gutiérrez*, 1994]

GUTIERREZ FRANCES, Mariluz. ***Notas sobre la delincuencia informática: atentados contra la Ainformación@ como valor económico de empresa***. En: Estudios de Derecho Penal Económico. Editores Luis A. Zapatero y Klaus Tiedemann. Ed. Univ. De Castilla-la Mancha, Tarancón (Cuenca), 1994.

[*Heredero*, 1992]

HEREDERO HIGUERAS, Manuel. ***La protección de los datos personales registrados en soportes informáticos. VISION GENERAL***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 2 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1992.

[*Hernando*, 1994]

HERNANDO, Isabel. ***La transmisión electrónica de datos (EDI) en Europa*** (Perspectiva jurídica). En: Actualidad Informática Aranzadi. A.I.A. Núm. 10 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Hernández*, 1996]

HERNANDEZ, Angel Gil. ***Protección de la intimidad corporal: aspectos penales y procesales***. En: Revista General del Derecho. R.G.D. Núm. 622-623. Jul-Ago, Valencia (Esp), 1996. Con el mismo título y contenido en Revista de Derecho Judicial. Escuela Judicial. C.G.P.J., Madrid, 1996.

[*Jiménez*, 1995]

JIMENEZ ESCOBAR, Raúl. ***Sobre la aplicación de la ley orgánica 5/92 a los ficheros automatizados de datos de carácter mantenidos por los abogados***. En: Revista Jurídica de Catalunya. R J.C. Núm. 1, Ed. Col.legi de Jurisprudéncia i legislación de catalunya. Director: Josep M. Vilaseco i marcet, Barcelona, 1995.

[*Jordán*, 1983]

JORDAN FLOREZ, Fernando. ***La informática jurídica (teoría y práctica)***. 10 ed., Universidad Piloto de Colombia. CII-UP., Bogotá, 1983.

[*Labilla*, 1997]

LABILLA RUBIRA, Juan José ***El fenómeno de las telecomunicaciones en la jurisprudencia del tribunal constitucional.*** En: Estudios de Derecho Judicial. Escuela Judicial. AOrdenación de las Telecomunicaciones@. C.G.P.J.No. VI, Madrid, 1997.

[*López*, 1997]

LOPEZ BLANCO, Carlos. ***El régimen jurídico de la telefonía en España.*** En: Estudios de Derecho Judicial. Escuela Judicial. AOrdenación de las Telecomunicaciones@. C.G.P.J.No. VI, Madrid, 1997.

[*López*, 1996]

LOPEZ DIAZ, Elvira***. El derecho al honor y el derecho a la intimidad. - Jurisprudencia y Doctrina***- . Ed. Dykinson, Madrid, (Esp.), 1996.

[*López*, 1993]

LOPEZ GARIDO, Diego. ***Aspectos de Inconstitucionalidad de la Ley Orgánica 5/1992, De 29 De Octubre***. En: Revista de Derecho Político. Univ. Nacional de Educación a distancia,, Núm. 38. UNED.Madrid, 1993.

[*López*, 1984]

LOPEZ-MUÑIZ GOÑI, Miguel. ***informática jurídica documental***. Ed. Díaz de Santos S.A.Bilbao, (País Vasco), España, 1984.

[*López*, 1993]

LOPEZ GARRIDO, Diego. ***Aspectos de inconstitucionalidad de la ley orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal***. En: Revista de Derecho Político. UNED. R.D.P. Núm. 38, Madrid, 1993.

[*López*, 1996]

LOPEZ ORTEGA, Juan José. ***Delitos socioeconómicos***. En: Estudios de Derecho Judicial. Escuela Judicial. AEstudios Sobre el Código Penal de 1995. Parte Especial@. C.G.P.J., Madrid, 1996.

[*Loreto*, 1992]

LORETO CORREIDORA, Ignacio Bell M. y PILAR COUSIDO, Alfonso. ***Derecho de la información (i). Sujetos y medios***. Ed. Colex, Madrid, 1992.

[*López*, 1993]

LOPEZ IBOR MAYOR, Vicente. ***Los límites al derecho fundamental a la autodeterminación informática en la ley española de protección de datos (LORTAD)***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 8 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1993.

[*Mangas*, 1996]

MANGAS MARTIN, Araceli. ***Las relaciones entre el derecho comunitario y el derecho interno de los Estados miembros a la luz de la jurisprudencia del Tribunal de Justicia.*** En: El Derecho Comunitario Europeo y su aplicación Judicial. Dirigida por Gil Carlos Rodríguez Iglesias. Ed. C.S.P.J. y la Universidad de Granada, Madrid, 1996.

[*Manzanares*, 1988]

MANZANARES, Henri y NECTOUX, Philippe. ***La informática al servicio del jurista***. Traducción de Elena Uribe Garros, Ed. Legis, Bogotá, 1988.

[*Marroig*, 1997]

MARROIG POL, Lorenzo***. Las instrucciones de la Agencia de protección de datos***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 23 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Martin*, 1996]

MARTIN-CASALLO LOPEZ, Juan José. ***Implicaciones de la Directiva sobre protección de datos en la normativa española.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 20 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1996.

[*Martin*, 1994]

MARTIN CASSALLO, Juan José. ***Agencia de protección de datos: qué es y qué finalidad persigue***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 13 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Martínez*, 1996]

MARTINEZ ARRIETA, Andrés. ***Tutela penal de la libertad de expresión.*** En: Cuadernos de Derecho Judicial. Escuela Judicial.Consejo General del Poder Judicial. C.G.P.J. No. XI, ADelitos contra la libertad y Seguridad@, Madrid, 1996.

[*Maronda, 1997*]

MARONDA FRUTOS, Juan Luis y TENA FRANCO, María Isabel. ***La informática jurídica y el derecho de la informática***. En: Revista General del Derecho. Año, II, Núm. 630, Marzo, Valencia (Esp.), 1997.

[*Mayor*, 1997]

MAYOR MENDEZ, Pablo. ***Las telecomunicaciones por satélite.*** En: Estudios de Derecho Judicial. Escuela Judicial. AOrdenación de las Telecomunicaciones@. C.G.P.J.No. VI, Madrid, 1997.

[*Menguez*, 1996]

MENGUEZ, José M. et all. ***Código Penal Español.*** 2a, ed., Comentarios, jurisprudencia, legislación. Ed. Colex, Madrid, 1996

[*Montoro*, 1991]

MONTORO PUERTO, Miguel. ***Jurisdicción Constitucional y procesos constitucionales.*** Tomo I y II Jurisdicción constitucional y procesos de control de la constitucionalidad. Procesos de protección de los derechos Fundamentales., Ed. Colex., Madrid, 1991.

[*Molina*, 1988]

MOLINA A. Carlos. ***Introducción a la criminología***. Ed. Biblioteca Jurídica, Medellín, 1988.

[*Moitinho*, 1996]

MOITINHO DE ALMEIDA, José Carlos. ***La protección de los derechos fundamentales en la jurisprudencia del tribunal de justicia de las Comunidades Europeas.*** En: El Derecho Comunitario Europeo y su

aplicación Judicial. Dirigida por Gil Carlos Rodríguez Iglesias. Ed. C.S.P.J. y la Universidad de Granada, Madrid, 1996.

[*Morales*, 1996]

MORALES PRATS, Fermín ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio***. En: Comentarios a la parte especial del Derecho Penal. Dirigida por Gonzalo Quintero Olivares y Coordinada por José Manuel Valle Muñiz. Ed. Aranzadi, Pamplona (Nav.), 1996.

[Morales, 1996]

MORALES PRATS, Fermín ***Protección penal de la intimidad, frente al uso ilícito de la informática en el Código penal de 1995.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, ADelitos contra la libertad y Seguridad@, Madrid, 1996.

[*Morales*, 1996]

MORALES PRATS, Fermín ***delitos contra la intimidad, en el código penal de 1995: reflexiones político-criminales.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, AEstudios del Código Penal de 1995@, Madrid, 1996.

[*Morales*, 1984]

MORALES PRATS, Fermin. ***La tutela penal de la intimidad: privacy e informática***. Ed. Barcelona (Esp.), 1984.

[*Muñoz*, 1996]
MUÑOZ CONDE, Francisco. ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio***. En: Derecho Penal-Parte Especial. Undécima edición. Ed. Tirant lo blanch, Valencia, 1996

[*Muñoz*, 1995]
MUÑOZ MERINO, Ana Muñoz. ***La evolución de la informática jurídica***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 16 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1995

[*Navarro*, 1998]
NAVARRO, Emilio del Peso. ***La seguridad de la información.*** En: Actualidad Informática Aranzadi. A.I.A.Enero 98, Ed. Aranzadi, Elcano (Navarra.), 1998.

[*Navarro*, 1996]
NAVARRO, Emilio del Peso. ***Resolución de conflictos en el intercambio electrónico de documentos.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Nora*, 1982]

NORA, Simón y MINC, Alain. ***Informe Nora-Minc. La informatización de la sociedad.*** Trad. Paloma García Pineda y Rodrigo Ruza, 1a., reimpresión. Ed. Fondo de Cultura Económica. México-Madrid-Buenos Aires, 1982.

[*Orti*, 1994]

ORTI VALLEJO, Antonio. ***Derecho a la intimidad e informática***. Ed. Comares, Granada (Esp.), 1994.

[*Orozco*, 1996]

OROZCO PARDO, Guillermo. ***Informativa y propiedad intelectual. Derechos.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 19 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996.

[*Páez*, 1995]

PAEZ MAÑA, Jorge. ***Comentarios sobre algunas particularidades en las bases de datos jurídicas***.. En: Actualidad Informática Aranzadi. A.I.A. Núm. 16 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1995.

[*Parejo*, 1996]

PAREJO, Luciano, JIMENEZ-BLANCO, A. y ORTEGA ALVAREZ, L. ***Manual de derecho administrativo***. Ed. Ariel, 4a., ed., Barcelona, 1996.

[*Pérez*, 1992]

PEREZ LUÑO, Enrique. ***A propósito de una obra de Mario G. Losano***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 2 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1992.

[*Pérez*, 1984]

PEREZ LUÑO, Antonio Enrique. ***Derechos humanos, Estado de Derecho y Constitución.*** Ed. Tecnos, Madrid, 1984.

[Pérez, 1996]

PEREZ VALLEJO, Ana María. ***La informática y el derecho penal***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 16 de Abril, Ed. Aranzadi, Elcano (Navarra.), 1996.

[Portero, 1996]

PORTERO GARCIA, Luis. ***Delitos cometidos por funcionarios contra las garantías individuales.*** En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J, Madrid, 1996.

[*Pritchard*, 1995]

PRITCHARD, Jhon. ***Información legal en la era electrónica: internet y los nuevos sistemas de comunicación.*** En: Revista Jurídica de Catalunya. R J.C. Edición Especial de Centenari: 1895-1995. Número Extraordinario. Ed. Col.legi de Jurisprudéncia i legislación de catalunya. Director: Encarna Roca i trias, Barcelona, 1995.

[*Queralt*, 1996]

QUERALT JIMENEZ, Joan J. ***Derecho penal español.*** Parte Especial, 3 ed., Ed. J.M., Bosch., Barcelona, 1996

[*Quilez*, 1993]

QUILEZ AGREDA, Ernesto. ***Sobre la inconstitucionalidad de la ley de protección de datos informáticos***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 8 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1993.

[*Ramos*, 1998]

RAMOS, Miguel Angel. ***Auditoria de la seguridad.*** En: Actualidad Informática Aranzadi. A.I.A.Enero 98, Ed. Aranzadi, Elcano (Navarra.), 1998.

[*Riascos*, 1997]

RIASCOS GOMEZ, Libardo O. ***La Constitución de 1991 y la informática jurídica***. Digitocomputarizado en 1991 y publicado por la Ed. Univ. de Nariño, UDENAR-UNED, Pasto (N), Colombia, 1997.

[*Riascos*, 1997]

RIASCOS GOMEZ, Libardo O. ***Los denominados recursos ante los Tribunales de Justicia de la C.E. y Andino.*** Digitocomputarizado en 1989 y publicado por la Ed. Univ. de Nariño, UDENAR-UNED, Pasto, 1997.

[*Riascos*,1996]

RIASCOS GOMEZ, Libardo. O. ***La criminalización de la actividad humana con aparatos de computación.*** En: Revista de Economia. Facultad de Economía, UDENAR, Pasto (N), 1996.

[*Riascos*, 1992]

RIASCOS GOMEZ, Libardo. O. ***El Thesaurus Jurídico***. Digitocomputarizada, Facultad de Derecho, UDENAR, Pasto (N), 1992.

[*Riascos*, 1989]

RIASCOS GOMEZ, Libardo O. ***Conferencias de informática jurídica***. Digitocomputarizada, Facultad de Derecho, UDENAR, Pasto (N), 1989.

[*Riascos*, 1983]

RIASCOS GOMEZ, Libardo. ***La Jurisdicción de Policía*** --Estudios sobre su constitucionalidad--- Tesis para optar título de abogado, Univ. de Nariño, Pasto, (Col.). 1983

[*Ribagorda*, 1996]

RIBAGORDA GARNACHO, Arturo. ***Seguridad de las tecnologías de la información***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Rigaux*, 1990]

RIGAUX, Fraçois. ***La protection de la vie privée et des autres biens de la personnalité.*** Bibliothèque de la Faculté de Droit de L´ Université Catholique de Louvain. Bruylant, Bruxelles, L.G.D.I., París, 1990.

[*Rodríguez*, 1993]

RODRIGUEZ IGLESIAS, Gil Carlos y LIÑAN NOGUERAS, Diego J. ***El derecho comunitario europeo y su aplicación judicial.*** Consejo General del Poder Judicial-Universidad de Granada, Ed. Civitas, 1a., ed., Madrid, 1993.

[*Romant*, 1996]

ROMANT R. José Luis. ***Peritaje en los delitos informáticos: problemas, lenguajes y criterios***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Romero*, 1984]

ROMERO COLOMA, Aurelia María. ***Derecho a la información y libertad de expresión. especial consideración al proceso penal***. Ed. Bosch, Barcelona (Esp), 1984.

[*Roig*, 1997]

ROIG, Agustín E. de Asís. ***La actividad sancionadora de la Agencia de Datos*** . En: Actualidad Informática Aranzadi. A.I.A. Núm. 22 de Enero, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Roig*, 1996]

ROIG, Agustín de Asís. ***Documento electrónico en la Administración Pública***. En: Cuadernos de Derecho Judicial. Escuela Judicial. Consejo General del Poder Judicial. C.G.P.J. No. XI, Madrid, 1996.

[*Ruiz*, l994]

RUIZ M, Carlos. ***L El derecho a la protección de la vida privada en la jurisprudencia del tribunal europeo de derechos humanos.*** Ed. Civitas, Madrid, 1994.

[*Ruiz*...,1997]

RUIZ-GIMENEZ CORTEZ, Joaquín. ***Artículo 10***. En: Comentarios a la Constitución Española de 1978. Dirigida por Oscar Alzaga Villaamil, Tomo II, Arts. 10 a 23. Editoriales de Derecho Reunidas. EDERSA, Madrid, 1997.

[*Sardina*, 1997]

SARDINA VENTOSA, Francisco. ***El derecho a la intimidad informática y el tratamiento de datos personales para la prevención del fraude.*** En: Actualidad Informática Aranzadi. A.I.A. Núm. 25 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1997.

[*Sempere*, 1997]

SEMPERE RODRIGUEZ, César. ***Artículo 18***. En: Comentarios a la Constitución Española de 1978. Dirigida por Oscar Alzaga Villaamil, Tomo II, Arts. 10 a 23. Editoriales de Derecho Reunidas. EDERSA, Madrid, 1997.

[*Serrano*, 1997]

SERRANO GOMEZ, Alfonso. ***Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.*** En: Derecho Penal- Parte Especial. Ed. Dykinson, 2a, ed., Colaboración de Alfonso Serrano Mailló, Madrid, 1997.

[*Souviron*, 1994]

SOUVIRON, José María. ***En torno a la juridificación del poder informativo del estado y el control de datos por la administración***. En: Revista Vasca de Administración Pública. R.V.A.P. No. 40, Sep-Dic., Bilbao (Esp.), 1994

[*Terredo*, 1995]

TERREDO, Federico. ***Protección jurídica de las bases de datos***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 16 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1995.

[*Torres*...,1995]

TORRES DEL MORAL, Antonio. ***Principios de derecho constitucional***. 2a., ed. Ed.Atomo editores, Madrid, 1995.

[*Vaquero*, 1985]

VAQUERO, Antonio y JOYANES, Luis. ***Informática***. Glosario de Términos y siglas-Diccionario de Inglés-Español. Ed. MacGraw-hill. Madrid 1985.

[*Van der*..., 1996]

VAN DER MENSBRUGGHE, Patricia. ***Flujos fronterizos de datos en la Directiva 95/46 de las Comunidades Europeas***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 20 de Julio, Ed. Aranzadi, Elcano (Navarra.), 1996

[*Valle,* 1996]

VALLE MUÑIZ, José Manuel, QUINTERO OLIVARES, Gonzalo y MORALES PRATS, Fermín. ***Delitos contra el patrimonio y contra el orden socioeconómico.*** En: Comentarios a la parte especial del Derecho Penal. Dirigida por Gonzalo Quintero Olivares y Coordinada por José Manuel Valle Muñiz. Ed. Aranzadi, Pamplona (Nav.), 1996.

[*Varela*, 1994]

VARELA CEA, Adolfo. ***Los derechos de los ciudadanos ante las nuevas tecnologías. Limites al uso de la informática en el sector privado***. En: Actualidad Informática Aranzadi. A.I.A. Núm. 13 de Octubre, Ed. Aranzadi, Elcano (Navarra.), 1994.

[*Vidal,* 1983]

VIDAL MARTINEZ, Jaime. ***El derecho a la intimidad en la Ley orgánica de 5-5-1982.*** Ed. Montecorvo S.A., Madrid, (Esp.), 1983.

[*Villaverde*, 1995]
VILLAVERDE MENENDEZ, Ignacio. ***Los Derechos del Público.*** Ed. Tecnos, Madrid, 1995.

[*Warren*, 1995]
WARREN, Samuel. ***El derecho a la intimidad.*** Edición a cargo de Benigno Pendás y Pilar Baselga. Ed. Civitas S.A., Madrid. 1995.

[*Wolveton*, 1985]
WOLVERTON, Van. ***El libro del MS-DOS-guía de Microsoft***- Ed. REI-ANDES, Educar, Bogotá, 1985.

[*WWW*]
WWW. UMONTREAL. EDU.CA (***Base de datos de la Universidad de Montreal*****).** Montreal (Canadá). 1997

[*WWW*]
WWW. AUSTLI.EDU.AU (***Base de datos de la Universidad de Australia*****).** 1997

[*WWW*]
WWW. RDH.GOV.CO (***Base de datos de la Red Nacional de Comunicación de Derechos Humanos)*****.** Presidencia de la República, Santafe de Bogotá, D.C.1997

[*WWW*]
WWW. MINJUSTICIA.GOV.CO (***Base de datos del Ministerio de Justicia de Colombia)*** **.** Presidencia de la República, Santafe de Bogotá, D.C. 1998.

[*WWW*]
WWW. ELTIEMPO.COM (***Base de datos del Diario El TIEMPO Colombia)*** **.** Santafe de Bogotá, D.C. 1998

[*WWW*]
WWW. ELMUNDO.ES/SU-ORDENADOR (***Base de datos del Diario El MUNDO España)*** **.** Madrid. 1998

[*WWW*]
WWW. UNIDUESSELDORF.DE (***Base de datos de la Universidad de Dusseldorf-Alemania).*** *1998*

CONCLUSIONES Y RECOMENDACIONES

1.1. El derecho fundamental de la intimidad personal y familiar, elevado a rango constitucional en la mayoría de las Constituciones Democráticas Occidentales, con el objeto de garantizar al máximo su protección y tutela por parte del Estado, así como la de los mismos particulares, desde sus orígenes más próximos a nuestra época hunde sus raíces en la dignidad, el respeto, el libre desarrollo y la inviolabilidad de la persona humana, tal como se planteo en el *Common Law* norteamericano, al abrigo del ensayo socio-jurídico de Warren y Brandeis, sobre *The Right to privacy* en 1890.

1.2. La proceso de conceptualización del derecho a la intimidad, a partir de los planteamientos vertidos sobre el *Right to privacy*, se elaboró en el ámbito mundial paulatinamente al abrigo de las directrices, normas y recomendaciones universales (Declaración de Derechos Humanos de 1948), legislaciones internacionales de ámbito europeo (Declaración de Derechos de Roma de 1950, El Convenio de Estrasburgo de 1981, Directivas de la UE: 95/46/CE y 97/66/CE, principalmente), legislaciones internacionales en el ámbito de los Estados Miembros de la ONU (Pacto de San José, Pacto de New York, etc); y por su puesto, de las legislaciones, trabajos doctrinales y jurisprudenciales de los diferentes Estados del Mundo. Este proceso de conceptualización del derecho ha servido para extraer sus elementos, las características, el contenido esencial y sus restricciones y limitaciones constitucionales y legales, más no una definición ponderada del mismo, pues estas han sido tan variadas como autores, épocas, sitios geográficos y convicciones políticas, religiosas, filosóficas, etc., de quienes han pronunciado o intentado su definición.

1.3. Las visiones o facetas del derecho de la intimidad, no son más que formas de desdoblamiento didáctico de un mismo derecho, y como tal, ayudan a la mejor comprensibilidad de esas características, contenido y limitaciones, a la vez, que ponen o quitan elementos de juicio para entender el significado mismo del derecho en un momento histórico concreto de su evolución. Por ello, las diferentes

visiones de un mismo derecho, *per se*, no crean nuevos derechos, a no ser que se escindan de forma que entre el derecho escindido y el derecho escíndente, apenas sólo quede el recuerdo de sus orígenes, más no de su estructuración, desarrollo, funcionamiento y ejercicio como derecho autónomo. La visión iusinformática del derecho a la intimidad, no es más que un desdoblamiento académico de aquél derecho devenido de la irrupción de las nuevas tecnologías de la información y la comunicación TIC y la informática; vale decir, cuando, por un lado, el ius (derecho) hizo contacto con llamada ciencia del manejo lógico, ordenado, concatenado de la información por medios informáticos, electrónicos y telemáticos (la informática) y formó la iusinformática o informática jurídica; y por otro, la información general o personal comenzó a ser objeto de la informática jurídica y la llamaron Adato@, para significar con ello que se trataba de una unidad de información codificada o tratada por medios informáticos, electrónicos o telemáticos.

1.4. La visión iusinformática no es una faceta exclusiva y excluyente del derecho de la intimidad, sino del conjunto de derechos fundamentales de la persona que permitan su desdoblamiento. Por ello, bien puede hablarse de la visión iusinformática del derecho al honor, a la honra, al buen nombre, a la propia imagen, etc. Esta particularidad globalizante, constituye un argumento más para desvirtuar que tal visión constituya un nuevo derecho y acreciente el planteamiento de que no es más que una faceta impuesta por el proceso de evolución tecnológica de los derechos fundamentales.

1.5. El Estudio y análisis de las diferentes legislaciones sobre protección del *Right to Privacy* (Caso de Canadá y Australia), de la protección de datos personales (Alemania, Australia, España, Estados Miembros de la UE) y de la protección del derecho de habeas data y de la información (Canada, Australia, Colombia), demuestran que la visión iusinformática del derecho a la intimidad, no tiene un origen unívoco en las diferentes regulaciones normativas internas e incluso internacionales, y a la vez, prueban que es aplicable al conjunto de derechos y libertades fundamentales (v.gr. Derecho a la libertad de expresión).

1.6. Los fundamentos de la visión iusinformática de los derechos y libertades fundamentales, incluido el de la intimidad, extractados del conjunto normativo universal, internacional e interno de los diferentes Estados, son: a) El derecho a conocer y ser notificado de todo tratamiento informatizado de los datos personales referidos a éste, tanto si son recolectados del titular o no; b) El derecho a la información sobre el tratamiento informatizado en todas, o en cada una de las etapas del proceso (recolección, almacenamiento, registro, conservación y comunicación), en tanto así se establezca en la legislación y las condiciones técnicas y jurídicas lo permitan; c) El tradicional derecho de acceso a la información por medios idóneos: informáticos, electrónicos y telemáticos; d) Ejercicio de las facultades estructurales del derecho de *habeas data* (conocimiento, actualización, rectificación y cancelación), unidas a las consecuenciales y de tipo técnico-jurídico de bloqueo, supresión, cancelación o borrado de datos. En definitiva el ejercicio del derecho de corte angloamericano expuesto por Westin: The Right to control information about oneself ; y f) El derecho de Oposición al tratamiento informatizado en las condiciones, circunstancias y eventos previstos en el ordenamiento jurídico.

2.1. El Discurso constitucional actual, se centra en si existe o no un nuevo derecho fundamental, como producto de la irrupción de las nuevas tecnologías de la información y la comunicación (TIC) e informática en el concepto de evolución de los derechos y libertades humanas. Para algunos la tensión-relación surgida entre la informática y las denominas *liberties pollution* del Common Law anglosajón, ha originado nuevos conceptos de libertades fundamentales del ser humano devenidas de las nuevas tecnologías, así sube a la palestra doctrinal y luego jurisprudencial del derecho español, la *libertad informática* para llenar un ámbito nuevo: la libertad que tiene toda persona para poder decidir en qué momento, para qué y por qué medios se recoge información por métodos informáticos, electrónicos y telemáticos y que sólo a él le concierne. Esta nueva libertad forma entonces, un nuevo derecho a la libertad informática. Para otros, la tensión-relación de la informática con los derechos fundamentales, confirma el camino de evolución de los derechos sin desvirtuarlos, aunque si transformarlos, al presentar nuevas visiones o facetas antes no descubiertas. Se sostiene así la vitalidad, la porosidad y la existencia transformada

de los derechos y libertades fundamentales con el paso del tiempo, a través de los desdoblamientos o visiones de un mismo derecho. Así se habla de visión iusinformática del derecho a la intimidad a la captación evolutiva de los fenómenos TIC e informática, como visión o faceta del derecho captador.

2.2. Una vez definidas las posturas sobre la existencia o no de derechos nuevos, a partir de bastiones de un derecho único, como sucede en España, con el derecho a la intimidad y el Auso de la informática@ (art.18.4 CE), se presenta a manera de ensayo constitucional la mejor ubicación de ese bastión del derecho a la intimidad (que también puede serlo del derecho al honor, a la imagen o al Apleno ejercicio de los derechos@), denominado del Auso de la informática@ como el de inviolabilidad de la persona a través de la utilización de medios informáticos, electrónicos y telemáticos. Guardando coherencia así con los anteriores bastiones de la intimidad, representados en la inviolabilidad de domicilio y la inviolabilidad de las comunicaciones (art. 18-2 y 18-3 CE). La inviolabilidad de la persona que tiene su epicentro en el art. 10 CE y art. 1 y preámbulo de la Const.Pol., es el fundamento constitucional de la visión iusinformática de los derechos y libertades fundamentales, y por su puesto del derecho a la intimidad. El antecedente remoto del principio de la inviolabilidad de la persona humana hunde sus raíces en el Common Law angloamericano, presentado en el mismísimo ensayo de Warren y Brandeis, sobre The Right to privacy, en el cual desde el siglo anterior hasta el presente el derecho a la privacy sin resquebrajarse sigue permaneciendo incólume fundandose en aquél principio constitucional, pero a la vez atento las innovaciones tecnológicas como las TIC e informáticas que revitalizan la existencia del derecho a la privacy y amplia sus visiones o facetas.

2.3. Abordamos finalmente un discurso constitucional y dialéctico sobre las diferentes denominaciones del llamado nuevo derecho a la libertad informática, como Aautodeterminación de la información@, Ainformática@ o Ainformática, el derecho a la Aintimidad informática@ y derecho de Ahabeas data@o Ahabeas scriptum@. Todo ello, para presentar el estado actual del debate sobre el nuevo derecho y paralelamente poder glosar al margen las diferentes posturas tanto en el ámbito constitucional doctrinal y jurisprudencial español como el colombiano. Cada

una de estas denominaciones del nuevo derecho, tienen su origen en las diversas fuentes normativas (art. 2.1 de la Constitución Federal Alemana, sobre el derecho a la información y el derecho al libre desarrollo de la personalidad), doctrinales como en el Common Law anglosajón (en la *liberties Pollution* por la tensión de la informática), en las fuentes doctrinales: italiana (ALa libertad informática@ como bien jurídico, según Frossini) y española (ALa libertad informática@ como nuevo derecho según Pérez Luño); así como jurisprudenciales tanto en Alemania (en el derecho alemán (Sentencia de 15 de Diciembre de 1983, Tribunal Federal Constitucional) como en Colombia (Corte Constitucional a partir de la Constitución de 1991). Con base en ese amplio como variopinto panorama sobre el nuevo derecho nos sirve de fundamento para defender la postura de la visión iusinformática de los derechos y libertades fundamentales, aplicando al margen el argumento *ad hóminem.*

3.1. Difícilmente, hoy por hoy, alguien puede negar la cascada de impactos que han producido las nuevas tecnologías de la información y la comunicación (TIC), junto con la informática jurídica en el plano de la investigación socio-jurídica, como en las más elementales actividades del ser humano de finales del siglo XX. Por esto, cada día se producen nuevas relaciones surgidas de la aplicación, uso, acceso y transferencia de información o datos de todo tipo, pero principalmente de carácter personal, por soportes, medios y aplicaciones informáticas, electrónicas y/o telemáticas. Esas nuevas relaciones entre los individuos o entre éstos y los Estados, como lo atesta en sus escritos por dispositivos electrónicos (Hipertexto y páginas WWW), el profesor Ethan de la Universidad de Montreal (Canadá), han ido delineándose al amparo de la llamada Acultura electrónica@ (electronic culture), que superando la cultura de la escritura y la impresión, suministra al hombre nuevas formas de comunicación, a partir de una lógica diferente, y por tanto, un replanteamiento del concepto tradicional de la información. Esa nueva lógica se estructura con medios o dispositivos de tipo electrónico, como las red de redes de información a través de computadores interconectados, la emisión y recepción de texto, imágenes y sonido por medios electrónicos y la aplicación, utilización y potenciación del hipertexto como mecanismo idóneo de información y comunicación electrónica.

3.2. En esta parte del trabajo, a título de ensayo, se propone con fundamento en la informática jurídica o iusinformática, las normas comunitarias, españolas y australianas que regulan el tratamiento informatizado de datos o información de carácter personal; en principio, una conceptualización, homologación y asimilación de términos utilizados frecuentemente en la legislación de los Estados, para significar o designar actividades eminentemente tecnológicas de aplicación diaria en el campo del derecho. Tales son los términos-instituciones jurídicas: AFicheros automatizados@, ABanco de información personal@, ABanco de datos@, ASoftware@, AHardware@, ASoportes, medios y aplicaciones@, AOrdenador o Computador@, ADatos o registros@, AArchivos o datos@, etc. Luego, también con el acercamiento de la terminología y la homologación se estudia, analiza las instituciones jurídicas que tienen un fundamento tecnológico, tales como: ADocumento electrónico de transferencia de datos@ o AEDI@

3.3. Especial atención y estudio se le brinda al denominado Electronic data interchange (EDI), por cuanto es el vehículo más idóneo actualmente para transmitir (emitir y recepcionar) datos de cualquier índole (voz, texto, sonido), carácter (personales, familiares, colectivos) o clase (generales o especiales v.gr. datos Asensibles@), a través de soportes, medios y aplicaciones informáticas, electrónicas o telemáticas, ya sea entre red de red de información locales (denominadas también Aintranet´s) o nacionales o internacionales (tipo internet´s). En la presente investigación se aborda el EDI dentro del concepto *Ethainiano*, es decir, en el ambiente de la cultura electrónica (AElectronic culture@), para luego aplicarlo al marco legislativo, jurisprudencial y doctrinal español y finalmente, conceptualizar y estructurarlo con base en el derecho público.

Una vez, logrado esto, comentamos algunos de los dispositivos de trasmisión electrónica de datos más utilizados por las personas naturales, jurídicas, públicas o privadas en los cuales se pone en evidencia y en juego el esquema paradójico que esta presente en toda la investigación: de un lado, la protección y garantía del Estados e incluso los particulares de los derechos, libertades públicas e intereses legítimos; y de otro, el alto riesgo de vulnerabilidad de los mismos, por Estado y

particulares. Esos dispositivos son: El correo electrónico (E-Mail), los foros de debate (The Newsgroups), los tablones electrónicos de anuncios (Electronic Bulletin Board System), las conferencias en tiempo real (Chat rooms); y, el Hipertexto (HTML): Páginas WWW.

3.4. Finalmente, proponemos con base en la estructura del ciclo informático del *habeas data o habeas scriptum*, propuesta por Frosini (en Italia) y Morales P., (en España), el procedimiento informático, electrónico o telemático de datos personales, compuesto de fases, etapas o ciclos ineludibles, con unos objetivos y finalidades generales y específicas. Dentro de las primeras, se hallan la determinación del procedimiento informático desde la etapa inicial (recolección, selección y organización) de datos, también llamada fase inicial o de *input de datos*, hasta las fases subsiguientes, tales como, la fase *in de datos* o fase propiamente informática, electrónica o telemática (que incluye una subetapas: almacenamiento, registro y conservación de datos); y la fase de salida de datos, o también conocida como fase output de datos (Subdividida en fase general y fase especial de salida de datos). Dentro de las segundas, podemos distinguir, entre otras, la implicación de los principios, derechos y deberes que orientan a las diferentes fases del procedimiento informático y previstos en el ordenamiento jurídico español, comunitario y australiano. Esta visión específica del procedimiento informático nos permite desvelar con mayor ahínco la visión iusinformática de los derechos fundamentales incluido el derecho a la intimidad, al tomar como punto de origen el derecho de habeas data y el derecho a la información previstos en los ordenamientos jurídicos antes mencionados.

4. 1. En el derecho público español la literatura jurídica sobre los derechos de la intimidad, de habeas data y de la información, es bastante amplia como fructífera. Las razones, entre otras, estriban en que los tres están íntimamente ligados en el tratamiento que les dispensa la doctrina, la jurisprudencia y el propio ordenamiento jurídico vigente. Igualmente, el estudio estrecho de aquéllos, se debe paradójicamente, al análisis que debe hacerse de la teoría de los límites constitucionales y legales, la preeminencia y ponderabilidad de los derechos fundamentales y la estructuración y vida propia de cada uno, sin afectar al núcleo

esencial del otro, sin desvirtuarlo, pero a la vez sin desaparecer como tal derecho en una eventual colisión. Equilibrio, ponderabilidad y autonomía de los derechos con respeto de los otros derechos, son las tesis más recurridas para explicar ese fenómeno paradójico. Y, es precisamente esto lo que se avizora en el inicio de la parte IV, de esta investigación.

4.2. El Derecho a la intimidad de las personas se aborda en esta parte del trabajo desde una de sus visiones: la iusinformática. La denominamos así, porque hace alusión al entronque que tiene el derecho a la intimidad con las nuevas tecnologías de la información y la comunicación (TIC) y la informática jurídica, como parte del conocimiento humano que tiene por objeto el estudio y análisis del acceso, tratamiento y transmisión de la información o datos, a través de medios automatizados, informáticos o telemáticos. La visión iusinformática de la intimidad, como se observa incorpora necesaria e indefectiblemente el estudio del habeas data (acceso, actualización, rectificación y cancelación de datos) y el derecho a la información (no sólo desde el ámbito negativo sino positivo: Asolicitar@ información), sin desconocer la estructura y autonomía constitucional y legal propias, pero a la vez, reconociendo que la visión sólo es explicable con la presencia y esencia de estos dos derechos también fundamentales o de la persona humana.

4.3. El planteamiento teórico-práctico de la estructuración de los llamados *Delitos informáticos*, tanto en la legislación española como colombiana, pretende llamar la atención de los iuspenalistas, sobre las nuevas tecnologías TIC y la informática, no simplemente desde un plano anecdótico, sino desde una concepción de la realidad actual que desborda el cumplimiento o no del principio *nullum crimen sine lege previa penale*, válido para postular o no la existencia de una conducta humana como típicamente punitiva, pero no para enfrentar la avalancha del fenómeno tecnológico que la *sociedad de la información* desde mediados del presente siglo convive con el significado de progreso, y a la vez, corre sus riesgos representados por esa especie de control tecnológico de carácter certero, penetrante, poroso e invisible. Claro está, que estos efectos de ventaja y de inconvenientes, no se solucionan si aparece o no en un Código Penal el *nomen iuris* de Delitos informáticos, aunque algunas legislaciones si lo han creído así, como hemos visto;

pero cuando menos se precisa y determina todas y cada una de aquellas figuras delictivas que estando bajo un bien jurídico distinto, como ocurre en España, se identifican por surgir de las nuevas tecnologías TIC y la informática. v.gr. la visión iusinformática de la intimidad en los delitos contra la intimidad; el daño informático en los delitos daños; la estafa informática en los delitos contra patrimonio social y económico; los delitos contra la autoría y derechos del software en los delitos contra la propiedad intelectual e industrial, etc. Aunque no están todos los que son, ni son todos los que están v.gr. los atentados informáticos contra el honor.

Esta identificación permite entender que el bien jurídico a proteger es pluricomprensivo y que tal vez no cabrían todas la figuras en un sólo título ni aún con varios capítulos, tal cual lo hiciera el legislador penal español de 1995, al desaconsejar al optar una técnica jurídico penal que desaconsejaba la unificación. Sin embargo, esta metodología refuerza el criterio del análisis y estudio doctrinal globalizante de los delitos llamados informáticos, pues la técnica jurídico penal seguida por el C.P.Esp., no elimina el análisis doctrinal e incluso jurisprudencial de esta clase aparte de delitos con identidad propia.

4.4. La explicación de la visión iusinformática del derecho a la intimidad para entender los llamados ADelitos contra la intimidad, el derecho a la propia imagen...@, prevista en el Título X, Capítulo I, ADel Descubrimiento y revelación de secretos@, del Código Penal de 1995, tiene como fin presentar un estudio limitado desde la órbita del derecho constitucional y administrativo y no estrictamente penal, a pesar de analizar conductas delictivas surgidas por los impactos de las nuevas tecnologías TIC y la informática.)Cómo es posible aquello?. Es factible, sí observamos lo siguiente: a) La legislación penal española eleva a rango de bien jurídico protegido el derecho constitucional a la intimidad, a partir del C.P.Esp., de 1995, pues aunque la doctrina iuspenalista desde el anterior Código había profusamente analizado la protección de la intimidad, en forma tácita, bajo Alos delitos contra la libertad y seguridad@, no fue si no hasta el vigente Código Penal que la protección se hizo expresa; b) Al protegerse la visión iusinformática de la intimidad, se aborda una gran parte del estudio nuevo para el derecho penal, el cual lo reduce al comentario de los Adelitos informáticos@, sin reconocer que existen,

más que en los comentarios de los doctrinantes nativos y extranjeros; c) El estudio de la visión iusinformática de la intimidad, implica un análisis contextual, tecnológico y de incardinación con otras ramas del derecho como el derecho constitucional y administrativo, y por su puesto del derecho penal y dentro del cual se aborda tan sólo una parte muy puntual, pues significa la última *ratio* con la que culmina el análisis de la mentada visión. Esto nos releva de cualquier puntualización doctrinal, legislativa e incluso jurisprudencial, sobre la totalidad de los delitos contra la intimidad y la propia imagen y por sustracción de materia, la de los delitos contra la Ainviolabilidad del domicilio@.

Aunque pudiera ser que en las futuras generaciones se planteara conductas delictivas de la visión iusinformática de la intimidad que vulneren la intimidad domiciliaria, con medios informáticos, considerando que el ordenador ubicado en cada domicilio o residencia, por ficción legal constituya domicilio y por tanto podríamos hablar de *violabilidad de la intimidad iusinformática del domicilio.* Sin embargo, hoy en día, por reiteradas sentencias de los Tribunales Supremo y Constitucional, se ha negado ficción legal iuris tantum, de domicilio a un vehículo (cualquier clase o tipo), menos se va a reconocer domicilio a un ordenador. Tecnológicamente resulta difícil pensar en tal posibilidad, máxime si se tiene en cuenta que una intercomunicación entre ordenadores, presenta un sinnúmero de posibilidades que hemos visto a lo largo del trabajo, que desvirtúan cualquier posibilidad, siquiera de determinación geográfica, pues un usuario puede estar en un punto X, el receptor en otro Y, el Servidor de la comunicación en un sitio Z, pero ni X ni Y, sujetos de la transmisión están en sus domicilios sino el uno en un sitio de trabajo y el otro en la universidad en equipos informáticos asignados por su condición de empleado y estudiante, respectivamente. Esta globalidad del fenómeno TIC y la informática, hace imposible la determinación de fronteras y límites geográficos de que precisa el domicilio.

4.5. Como colofón tratamos doctrinalmente la estructuración del *delito de los datos personales registrados en forma automatizada contra la intimidad en el Código Penal Español de 1995*. Este específico delito surge del análisis y estudio de la visión iusinformática de la intimidad, el auxilio de la informática jurídica documental, y las teorías jurídico penales vertidas sobre los delitos contra la intimidad con medios informáticos, como han preferido en llamarlos quienes no reconocen ni siquiera doctrinalmente la existencia de los *delitos informáticos*. La figura se analiza utilizando terminología propia del tratamiento automatizado de datos que en algunas partes se identifica con los términos asignados por el legislador penal a los tipos básicos, agravados o atenuados contenidos en el Capítulo I, del Tit. X., del C.P.Esp., de 1995. En efecto, la figura típica consiste en el *acceso, utilización, alteración e interceptación de datos contenidos en documentos informáticos*. Esta figura se disecciona y desdobla, así: a) Parte *ab initio* del tipo: acceso, utilización y alteración; b) Parte *in fine* del tipo: la interceptación o

intervención. Esto permite, puntualizar el *iter* del tratamiento automatizado de la información o datos, tal como esta previsto en la legislación llamada extrapenal (LORTAD, Directivas Comunitarias 95/46/CE, entre otras), así como el entendimiento del concepto de *documento informático, electrónico o telemático* , según la legislación iusadministrativista y tributaria, pioneras en el tema y como tal sus enseñanzas hermenéuticas son válidas para todas las ramas del derecho (principalmente, arts. 37 y 45 de la LRPJA, R.D.No.263/1996; Ley 28/1992, R.D. 2402/1992).